Robust Logo Watermarking

By:

Mohammad Barr

A thesis submitted in part fulfilment of the degree of Doctor of Philosophy.

Under the supervision of:

Dr. Cristian Serdean

School of Engineering and Sustainable Development

De Montfort University

Leicester

June 2018

Abstract

Digital image watermarking is used to protect the copyright of digital images. In this thesis, a novel blind logo image watermarking technique for RGB images is proposed. The proposed technique exploits the error correction capabilities of the Human Visual System (HVS). It embeds two different watermarks in the wavelet/multiwavelet domains. The two watermarks are embedded in different sub-bands, are orthogonal, and serve different purposes. One is a high capacity multi-bit watermark used to embed the logo, and the other is a 1-bit watermark which is used for the detection and reversal of geometrical attacks. The two watermarks are both embedded using a spread spectrum approach, based on a pseudo-random noise (PN) sequence and a unique secret key. Robustness against geometric attacks such as Rotation, Scaling, and Translation (RST) is achieved by embedding the 1-bit watermark in the Wavelet Transform Modulus Maxima (WTMM) coefficients of the wavelet transform. Unlike normal wavelet coefficients, WTMM coefficients are shift invariant, and this important property is used to facilitate the detection and reversal of RST attacks.

The experimental results show that the proposed watermarking technique has better distortion parameter detection capabilities, and compares favourably against existing techniques in terms of robustness against geometrical attacks such as rotation, scaling, and translation.

ACKNOWELDGMENTS

I would like to thank my supervisor Dr. Cristian Serdean for his guidance and patience in this long and difficult journey of PhD. His guidance is the key behind the completion of this thesis. It would not have been possible without his continuous support.

It is the prayers of my parents, my brother, and my sisters that did not let me give up and made me work harder. I would also like to thank my wife who was with me during this difficult journey and whose patience and encouragement kept me motivated to finish my thesis.

Lastly, I would like to express my gratitude to the Saudi government and especially the Saudi Cultural Bureau for their generous financial support during this whole period. Without their support, I would not have been able to complete this thesis.

Table of Contents

List of Figures

List of Acronyms

ABC	Artificial Bee Colony
AC	Alternating Current
AEAD	Average Edges Angles Difference
AT	Arnold Transform
AWGN	Additive While Gaussian Noise
BER	Bit Error Rate
BPP	Bits Per Pixel
CAGR	Compound Annual Growth Rate
CQ	Correlation Quality
CSF	Contrast Sensitivity Function
dB	Decibel
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DMWT	Discrete Multi-Wavelet Transform
DWT	Discrete Wavelet Transform
ESDR	Edges Standard Deviation Ratio
FFT	Fast Fourier Transform
FMT	Fourier-Mellin Transform
FNR	False Negative Rate
FPR	False Positive Rate
GA	Genetic Algorithms
HH	High-High Sub-Band
HL	High-Low Sub-Band
HVS	Human Visual System

IDWT	Inverse Discrete Wavelet Transform
JPEG	Joint Photographic Experts Group
LH	Low-High Sub-Band
LL	Low-Low Sub-Band
LSB	Least-Significant-Bit
MLM	Maxima Location Mean
MOS	Mean Opinion Score
MPEG	Motion Picture Experts Group
MRA	Multi-Resolution Analysis
MSE	Mean Square Error
NCC	Normalized Cross-Correlation
NSST	Non-Subsampled Shearlet Transform
PHT	Polar Harmonic Transform
PRN	Pseudo-Random Number
PSNR	Peak Signal to Noise Ratio
QR	Quick Response Code
RGB	Red, Green, Blue
ROI	Region of Interest
RST	Rotation, Scaling, Translation
SIFT	Scale Invariant Feature Transform
SNR	Signal-to-Noise Ratio
SSIM	Structural Similarity Index
SVD	Singular Value Decomposition
WNR	Watermark-to-Noise Ratio
WTMM	Wavelet Transform Modulus Maxima

CHAPTER 1: INTRODUCTION

1.1 Background

Nowadays, digital multimedia content (and in particular, image data) is widely available and is frequently distributed over the Internet. Copyright protection of such content is important to ensure its rightful ownership and legal distribution. Thus, storing the ownership information within the digital data itself has emerged as an active area of research.

Digital Watermarking is a valuable tool which enables the hiding or embedding of a signal (usually containing ownership information) into another signal (usually image or video content). It can be used to protect digital data against copyright infringement [1]. Important applications of watermarking include broadcast monitoring, owner identification, proof of ownership, authentication, fingerprinting, copy control and covert communications [2]. In particular, watermarking can be successfully used in the following areas:

- ***Broadcasting:*** where broadcasters can use watermarking to track and verify TV programs and advertisements,
- ***Entertainment:*** where movie studios can detect and deter piracy of movies. Similarly, watermarks can also be used to secure the distribution of digital cinema content,
- ***Banking:*** where central banks can use watermarks to prevent digital counterfeiting of currency notes,
- ***Photography:*** where photographers can identify and manage the copyright of their photographs, and can embed additional metadata,
- ***Government Organizations:*** where watermarking can be used to authenticate employee IDs, to prevent theft, fraud and counterfeiting of important documents.

The global digital watermarking market has seen a continuous growth over the past few years and the growth is expected to also continue in future. For example, in 2015, the

global watermarking market was worth USD 1.0663 Billion while by 2020, it is forecasted to grow by approximately 300% i.e. to around USD 2.8989 Billion [3].

This translates to a compound annual growth rate (CAGR) of 22.1% from 2015 to 2020. The healthy and sustained growth of digital watermarking market shows a continued interest of stakeholders in watermarking technology.

An important problem related to watermarking is that it is not sufficient just to store the ownership information, but also to hide it and separate it from the real data and to protect it against tampering. It is to be noted that watermarking is very much different from encryption. While, they both provide protection of the data, encryption only provides protection during transmission. The data is not protected once it is decrypted. On the other hand, a watermark is always present in the data [4].

A watermark exhibits several characteristics. Among others, these include: robustness and tamper resistance, transparency, capacity, fidelity, computational cost, and false positive rate [2]. Robustness is the characteristic of a watermark that indicates how well the watermark can survive common signal processing operations such as lossy compression. Tamper resistance can be further classified into four types: resistance against active, passive, collusion or forgery attacks. The various types of attacks are discussed further in Chapter 2. Fidelity refers to the ability of a watermark to embed into another signal without visibly changing that signal. Computational cost usually determines the computational resources, speed, or time required to embed the watermark or to recover and determine the authenticity of the watermark. Lastly, the false positive rate is the rate at which the watermark is detected in a signal even when the signal does not contain the watermark. An ideal watermark should be robust, tamper resistant, have high fidelity, small computational cost and a zero false positive rate. However, due to the various constraints in the real world, this is not always possible and usually compromise is made on one or more of these characteristics when watermarking is used in real world applications. To address the above issues, different methods have been proposed in the literature. These methods can be broadly classified into two categories: spatial domain methods and transform domain methods.

Spatial domain methods are easy to implement but are typically less robust against attacks. On the other hand, transform domain methods are more complex compared to the spatial domain methods, but they are relatively more robust [1]. A detailed discussion of these methods is presented in Chapter 2.

1.2 Scope

The main goal of robust logo watermarking and of this research is to protect intellectual property of copyrighted materials distributed by third parties, by hiding a perceptually invisible logo in the host content. The watermarking technique should be robust to intentional and unintentional attacks such as image compression, image manipulation, noise addition, loss during transmission, etc. The aim is to maximize the capacity and robustness of the watermark while at the same time preserving its invisibility.

The watermarking technique should be designed in such a way that third parties cannot change or remove the watermark. The watermark should be very difficult to remove without destroying the watermarked host image in the process.

A literature survey is carried out to establish previous relevant research into robust (logo) watermarking algorithms. Various algorithms and techniques are investigated in order to achieve the above requirements and improve on the existing techniques.

1.3 Aims and Objectives

The main aim of this work is to propose a novel blind logo watermarking technique for RGB images, which is robust to geometrical transforms. This aim is achieved with the help of the following objectives:

a. Investigate spread spectrum based techniques for robust (logo) image watermarking.
b. Investigate the effect of spatial and transform domain methods for robust (logo) image watermarking.
c. Investigate the use of Discrete Wavelet Transforms (DWT) and Discrete Multi-Wavelet Transforms (DMWT) for (logo) image watermarking of colour (RGB) images.

d. Investigate the use of Wavelet Transform Modulus Maxima (WTMM) to achieve robustness against geometrical attacks, and in particular robustness against RST attacks.
e. Investigate robustness to different types of attacks and evaluate the performance of the proposed technique.

1.4 Thesis Outline

The remaining part of the thesis includes six chapters.

In Chapter 2**,** fundamental concepts of watermarking are presented. These include the components of a watermarking model, classification of watermarking schemes, properties of a watermark, applications of watermarking, types of attacks, and classification of watermarking techniques. In Chapter 3, a literature survey of the different robust watermarking methods is presented. These include both spatial and transform domain techniques. Moreover, frequently used spread spectrum techniques have also been reviewed and the differences between the existing spread spectrum techniques and the proposed technique have been highlighted. Wavelet transform modulus maxima and related concepts are introduced in Chapter 4. This is followed by a description of the proposed novel watermarking scheme in Chapter 5. A discussion of the experimental results of the proposed method are presented in Chapter 6. Finally, conclusions drawn from this work are presented in Chapter 7.

CHAPTER 2: FUNDAMENTALS

There are several ways to perform watermarking of multimedia content. Usually multi-bit information is invisibly embedded, in host content such a song, text, a movie or a picture. Watermarking can be carried out in the spatial domain as well as in the transform domain, and various transforms have been proposed and used over time. The watermark should be imperceptible, in order to preserve the quality of the watermarked content, and various human visual models have been proposed to address this. Robustness and imperceptibility are the key concerns when watermarking quality is judged. Depending on the application, watermarking capacity is also a key factor. A general solution for increasing robustness is to embed the watermark with higher power. However, this impacts on invisibility, so any watermarking scheme needs to achieve a trade-off between robustness, capacity and the invisibility of the watermark. Various techniques have been proposed to achieve this (e.g., [4], [5], [6], and [7]). Generally, spread-spectrum modulation based techniques (e.g., [8], [9]) are frequently used due to their inherent noise-like nature and their ability to securely spread the watermark in the entire image content. Another frequently used technique is quantization watermarking [10], [11], and [12].

2.1 Components of a Basic Watermarking Model

The fundamental components of a digital watermarking process include [13]:

- **Watermark generation:** It refers to the process of generating a suitable watermark for an application. Watermark generation and the very size and type of the watermark are usually constrained by the properties required in a given application. For example, in a copyright protection application, a watermark may need to be able to withstand common signal and image processing operations. Hence, the watermark's robustness needs to be considered while selecting a watermark which would be suitable for such applications.

- **Watermark embedding:** It refers to the process of finding a suitable method and location for the embedding or insertion of the watermark in the host multimedia content (e.g., a digital image).
- **Watermark detection:** It refers to the process of detecting the watermark that has been embedded in the host multimedia content. This will allow one to establish the authenticity and/or the ownership of the content.

2.2 Classification of Watermarking Schemes

Watermarking schemes can be classified in many ways. Some of these are as follows:

- **Symmetric vs Asymmetric Watermarking:**

  Symmetric watermarking schemes use the same key for the embedding and the detection of the watermark. A requirement of these schemes is that they require the key that is used for watermark embedding to be available at the watermark detector. This can potentially lead to a security problem such as the removal of the watermark. On the other hand, Asymmetric watermarking schemes use different keys for the embedding and the detection of the watermark. In these schemes, a private key is used for embedding the watermark while the detector is only aware of a public key. This arrangement makes it impossible or extremely difficult to rely on compromising a key in order to remove the watermark.
- **Robust, Semi-fragile, and Fragile Watermarking:**

  Watermarks can be classified into three categories based on their robustness property. These are: robust, semi-fragile, and fragile [17]. Robust watermarks are designed to be resilient to attacks and very difficult to remove. On the other hand, semi-fragile watermarks are capable of partially tolerating changes to the watermarked image (e.g., the addition of quantization noise from lossy compression). Lastly, fragile watermarks are meant to be easily destroyed if the watermarked image is manipulated even slightly.
- **Spatial Domain vs Transform Domain:**

  Spatial domain methods are simple techniques that involve direct modification of pixel intensities. They commonly involve additive watermarking techniques as

well as Least Significant Bit (LSB) modification techniques in which the least significant bit of each bit-plane is modified [20]. The main advantages of spatial domain watermarking techniques lie in their simpler implementation and lower computational time complexities while the main drawback of these techniques is that they tend to offer lower watermark capacity and be less robust to attacks [21]. On the other hand, transform domain techniques insert information into transform coefficients. These methods are discussed in detail in Section 2.6.

2.3 Watermarking Properties

- **Perceptual similarity (Imperceptibility):** Achieving visual imperceptibility means that even though the content of an image will change as a result of embedding the watermark, visually, the difference is unnoticeable.

  Several metrics can be employed to evaluate the perceptual similarity. These can be broadly classified into methods based on objective and subjective criteria. While methods based on objective criteria use mathematical formula to quantify the perceptual similarity, subjective methods mainly rely on the opinion of the users. Correlation quality (CQ), peak signal to noise ratio (PSNR), mean square error (MSE) and structural similarity index (SSIM) are some of the examples of objective methods while Mean Opinion Score (MOS) is one of the most commonly used subjective methods for the evaluation of image quality/similarity.
- **Visibility:** A visible watermarking scheme is a scheme that allows the watermark to be visible on the object in which it is embedded. Its use can be in displaying a company logo, etc.

  Hence, watermarking schemes can be classified as either ‘visible’ or ‘invisible’ based on the appearance of the watermark on the image.

  It is important to differentiate between ‘perceptual similarity’ and ‘visibility’. They can be easily confused with each other because of their similarities.

  However, while ‘perceptual similarity’ aims to reduce the perceptual difference between images before and after watermarking, ‘visibility’ aims to make the watermark appear on the image with a strength that can normally be controlled. Thus ‘visibility’ results in a perceptual difference between images before and

after watermarking. By in large, the main focus of research has been on invisible watermarking schemes.

- **Blind embedding/retrieval:** Blind embedding/retrieval is a property that defines the computational independence on the original information or its derivatives to retrieve the required watermark information. A watermarking scheme can be categorized as a blind, semi-blind, or non-blind.

  A blind watermarking scheme requires no original input image or any information derived from it in order to recover the embedded watermark. On the other hand, a semi-blind watermarking scheme often refers to the schemes that can operate objectively without the original image and its derived information, but still require the original image. Lastly, non-blind watermarking schemes require the original image in order to be able to recover the watermark [13].
- **Invertibility:** Invertibility is the property that defines whether a watermarked image can be restored to its original version without leaving any embedding distortion behind.
- **Robustness:** Robustness has been defined differently by different authors. For example, according to Piper and Safavi-Naini [14], a robust watermarking scheme is the one that can detect watermark in a 'processed' image. On the other hand, Cox et al. [15] define it as the ability to detect the watermark after common signal processing operations. Hence, keeping in view both these definitions, robustness can be defined as the degree to which a watermarking scheme can resist modifications to the watermarked image.

  These modifications can be either intentional in the form of attacks designed to render the watermark undetectable, or unintentional, such as the side effect of performing various common signal processing operations such as compression.
- **Embedding capacity:** It refers to the amount of watermarking data that can be (robustly) embedded without compromising on the perceptual similarity of the watermarked and the non-watermarked image.

  Capacity estimation of watermarking is an active area of research. It is usually expressed in terms of the number of bits or the number of bits per pixel (bpp).

- **Error probability:** Error probability defines the reliability of a watermarking scheme. Commonly used metrics for determining the error probability of a watermarking scheme are bit error rate (BER), false positive rate (FPR), and false negative rate (FNR). BER may be improved by using suitable error correction codes to protect the watermark.
    - **Bit error rate**: It is defined as the number of bits in error divided by the total number of bits.
    - **False positive rate**: It can be defined as the rate at which an algorithm falsely detects a watermark though in reality the watermark is not present.
    - **False negative rate:** It can be defined as the rate at which an algorithm fails to detect the watermark even though the watermark is present.

  A zero FPR and FNR represents an ideal or very reliable detection. However, this may not be achievable in practice due to attacks. Hence, the aim in watermarking applications is usually to achieve a low FPR and FNR as well as achieving a very low BER (e.g., of the order of 10^{-6}).

- **Normalized Cross-correlation coefficient:** The normalized cross-correlation (NCC) coefficient of two images is a measure of similarity between the two images. It is generally used to evaluate the quality of a recovered watermark.
  The NCC $\gamma\ (u, v)$ of an image 'f' with coordinates 'x' and 'y' and its template 't' with its coordinates 'u' and 'v' can be computed as in Eq. (1) [16].

$$\boldsymbol{\gamma(u,v,)} = \frac{\sum_{x,y}[\boldsymbol{f(x,y)}-\bar{\boldsymbol{f}}_{\boldsymbol{u,v}}][\boldsymbol{t(x-u,y-v)}-\bar{\boldsymbol{t}}]}{\left\{\sum_{x,y}[\boldsymbol{f(x,y)}-\bar{\boldsymbol{f}}_{\boldsymbol{u,v}}]^{\boldsymbol{2}}\sum_{x,y}[\boldsymbol{t(x-u,y-u)}-\bar{\boldsymbol{t}}]^{\boldsymbol{2}}\right\}^{\boldsymbol{0.5}}} \quad (1)$$

In Eq. (1), $\bar{t}$ is the mean of the template and $\bar{f}_{u,v}$ is the mean of $f\ (x, y)$ in the region under the template.

Among these properties, imperceptibility, robustness, and capacity are generally the more important properties of a watermarking scheme. Ideally, a watermark should achieve all

three properties at the same time, but practically, this is often not possible. A trade-off has to be made among these constraints as they are generally conflicting requirements.

The trade-off is generally made on the basis of the requirements of each specific watermarking application. A possible trade-off is shown in Figure 1.

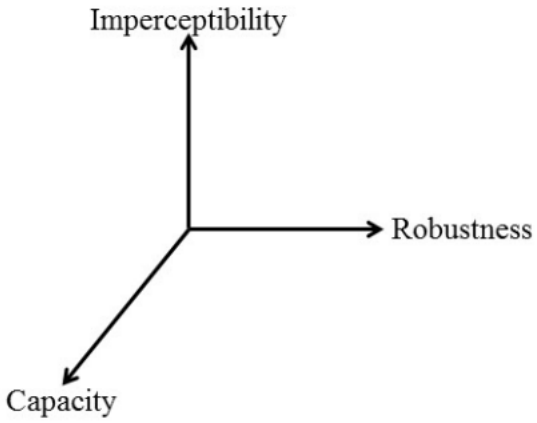


Figure 1 Possible trade-off between constraints

Generally, among the above properties, imperceptibility is of very high importance. That is because the artefacts produced during the process of watermark embedding are both annoying and undesirable.

Moreover, they may also compromise the commercial value of the image. Robustness is another important property of a watermark. Unfortunately, increasing robustness often implies some perceptual degradation. On the other hand, improving imperceptibility imposes limitations on robustness. Similarly, increasing capacity (i.e. the ability to hide a larger amount of information) limits the robustness of the watermark while increasing robustness limits the capacity of the watermark. As a result, imperceptibility, robustness and capacity are opposing constraints which cannot be all achieved at the same time. Hence, usually, a trade-off is made based on the importance of each of these factors with respect to the target application.

2.4 Applications of Watermarking Techniques

Watermarking can be useful in a number of applications. Each target application has its own set of constraints and requirements. It is not possible to address all watermarking properties for every algorithm. Rather, it is more sensible to identify a target application first, identify its constraints, and then design a practical watermarking scheme which works under those constraints.

Watermarking applications can be classified into five broad categories [18]: protection of intellectual property rights, content verification, information hiding, and annotation. A brief description of each application category is presented below:

- **Protection of Intellectual Property Rights:** The purpose of watermarking schemes aimed at this class of applications is to convey information about content ownership and intellectual property rights.
  Application scenarios in this class include copyright protection, copy protection and fingerprinting, and rely on robust watermarks.
- **Content Verification:** The purpose of watermarking schemes aimed at this class of applications is to ensure that the original multimedia content has not been altered by a third party. Moreover, they can also aim to determine the type and location of alteration. Application scenarios in this class include authentication and integrity checking. Such applications rely on fragile watermarks.
- **Information Hiding:** The purpose of the embedded watermark in a watermarking scheme aimed at this class of applications is to offer a side channel used to carry additional information. Application scenarios include, system enhancement and secret communications.
- **Annotation:** The purpose of watermarking schemes aimed at this class of applications is to convey the object-specific information to users of the media. For example, augmented contents, multimedia indexing, content based retrieval, patient record identification for medical images, etc.
- **Broadcast Monitoring:** Advertisers are generally interested in making sure that they receive the airtime that they have paid for. Similarly, artists and musicians

are also interested in making sure that they receive royalty amounts corresponding to the actual air time. Watermarks can be used for broadcast monitoring by embedding a watermark in each advertisement or other media content. Monitoring stations can then be used to receive the broadcast content and identify the time and location of the broadcast of the relevant content [19].

2.5 Watermarking Attacks

Any malicious attempt to perform unauthorized embedding, removal, or detection of a watermark can be termed as a watermarking attack [13]. Watermarking attacks are often dictated by the capabilities and the needs of the adversary.

Attacks on watermarking can be broadly classified into two types: active and passive.

2.5.1 Active attacks

An active attack involves unauthorized embedding and/or unauthorized removal of the watermark. These attacks usually attempt to alter the watermarked image in one way or another.

Active attacks can be categorized in the following types:

- **Elimination**: In an elimination attack, an adversary tries to generate an output image, which is perceptually similar to the watermarked image but for which the watermark is no longer detected. These methods aim to completely remove the watermark from the watermarked image.
- **Collusion**: In a collusion attack, an adversary has access to multiple copies of the same host data each watermarked with a different watermark. This information can be used to compromise the embedded watermarks by averaging all copies together to obtain a close approximation of the original image.
- **Masking**: Masking attacks do not actually remove the watermark but make it undetectable to the detectors.
- **Distortion**: The attacks aim to distort the watermark to make it undetectable. De-noising and desynchronization attacks are two subclasses of distortion attacks. Rotation, scaling, and translation (RST) and affine transforms are common geometric attacks that can be used to distort watermarks.

- **Forgery**: In a forgery attack, an adversary or unauthorized person attempts to embed a valid watermark of their own in an attempt to claim false ownership of the watermarked multimedia content.
- **Copy**: This attack is similar to a forgery attack but in this case the attacker copies a watermark from one valid watermarked image to another in order to falsely authenticate an invalid watermarked image.
- **Ambiguity**: An ambiguity attack is aimed at making the detection process ambiguous and thus allowing even an invalid watermark to pass as a valid one.
- **Scrambling**: These attacks aim to scramble the samples of the watermark before passing it through a detector, in order to avoid detection. The samples of the watermark are later on descrambled before using the host content. A typical example of a scrambling attack is the mosaic attack.

2.5.2 Passive attacks

A passive attack involves unauthorized detection of the watermark. These attacks are aimed at knowing the presence or absence of the watermark.

- **Detection only:** In these attacks, an attacker only detects the presence of a valid watermark in a watermarked image.
- **Incision detection:** In these attacks, apart from detection of the watermark in a watermarked image, the attacker can distinguish the watermark from that of other watermarked images.
- **Comprehensive detection:** In these attacks, the attacker not only knows the presence of the watermark and can distinguish it from other watermarked images, but also obtains information, at least partially, about the content carried by the watermark, without modifying the watermarked image.

2.6 Transform Domain Watermarking Schemes

As discussed in Section 2.2, transform domain techniques insert information into transform coefficients. Many types of transforms have been used for this purpose such as: Fourier transforms [22] and fractional Fourier transforms [23], Cosine transforms [24], Wavelet transforms [25], fractional Wavelet transforms [26], fractional dual tree complex Wavelet transforms, Hadamard transforms, Curvelet transforms, and Singular Value Decomposition (SVD) transforms [27]. Amongst these, Cosine transforms and Wavelet transforms tend to be more frequently used. Generally, transform domain techniques provide higher imperceptibility and robustness to attacks but are more complex to implement and have higher computational complexity. Some of these transforms benefit from established Human Visual System (HVS) models that can be very useful in a watermarking scheme.

2.6.1 Discrete Cosine Transform

The Discrete Cosine Transform (DCT) transforms an image from spatial or pixel domain to frequency domain. It is an important transform mainly because of its energy compaction property which allows it to store most of the information in very few (low-frequency) coefficients. Because of its good energy compaction performance, it has been adopted in image compression standards such as Joint Photographic Experts Group (JPEG) as well as in many Motion Picture Experts Group (MPEG) video compression standards.

Forward DCT is used to transform the image into DCT coefficients, while inverse DCT is used to reconstruct the image back from the transform coefficients. Mathematically, the DCT is defined as:

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (2)$$

where

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}} \; if \; u = 0 \\ 1 \; if \; u > 0 \end{cases} \quad (3)$$

Here $p\,(x,y)$ is the pixel at position (x,y) of the image. N is the size of the block on which the DCT is applied.

Commonly, the DCT is applied on small 8x8 size blocks, as shown in Figure 2. Here, $N = 8$, so Equation (1) reduces to:

$$D(i,j) = \frac{1}{4}C(i)C(j)\sum_{x=0}^{7}\sum_{y=0}^{7}p(x,y)\cos\left[\frac{(2x+1)i\pi}{16}\right]\cos\left[\frac{(2y+1)j\pi}{16}\right] \quad (4)$$

Similarly, the inverse DCT can be obtained using the following relationship:

$$p(i,j) = \frac{1}{4}\left[\sum_{x=0}^{7}\sum_{y=0}^{7}C(i)C(j)D(i,j)\cos\left[\frac{(2x+1)i\pi}{16}\right]\cos\left[\frac{(2y+1)j\pi}{16}\right]\right] \quad (5)$$

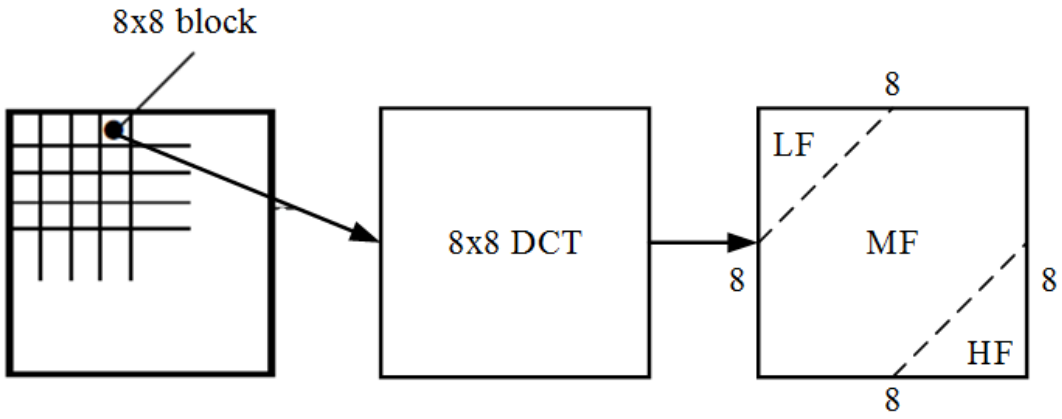


Figure 2 Applying DCT on an image

It can be seen from Figure 2 that after applying DCT, the Low Frequency (LF) content is represented by transform coefficients in the top-left corner of the DCT matrix, the High Frequency (HF) content is represented by transform coefficients in the bottom-right corner of the DCT matrix while the Medium Frequency (MF) content is represented by the remaining transform coefficients.

It is also important to note that due to the block based structure of DCT, blocking artefacts are commonly associated with it. However, in the context of watermarking, DCT is associated with good perceptual invisibility and acceptable robustness against JPEG compression [20].

2.6.2 Discrete Wavelet Transform

The Discrete Wavelet Transform (DWT) is another important tool for signal analysis. It shares some similarities with the Discrete Fourier Transform (DFT). For example, both DWT and DFT represent a signal through a linear combination of their basis functions. But, for DFT, the basis functions are dilations of sinusoidal signals (sines and cosines, or just cosines for the DCT transforms) with each of the sinusoids spanning the entire time interval. On the other hand, for the DWT, the basis functions are different translations and dilations of a 'Mother' wavelet along with a scaling function. Unlike DFT, for DWT, each basis function spans a reduced sub-interval. Both DFT and DWT provide frequency localization through the dilations of their basis functions. Hence, both DFT and DWT can be used to analyse frequency information about a signal. However, the basis functions of DFT are not finite and hence the DFT does not provide time localization. On the other hand, the basis functions of DWT are compact and finite and as such the DWT can provide time localization (or localization in space for the 2D case) as well. Hence, the DWT can be used to obtain both time (or space) and frequency information about a signal while DFT is limited to only providing frequency information about a signal.

In DWT, a signal is decomposed into a set of basis functions called 'wavelets'. These wavelets can be obtained from the 'mother wavelet' using techniques known as dilation and shifting. Mathematically, this process can be represented using the following relationship:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) \tag{6}$$

Here a is the dilation (scaling) parameter and b is the shifting parameter.

Theoretically, the number of types of mother wavelets can be infinite [28] but in practice the number of mother wavelets is relatively limited. It is important that the selected type and order of the filter closely matches the characteristics of the target signal. The order of a wavelet determines the smoothness and compactness of the wavelet. For example, the higher order wavelets are smoother but less compact in time. Generally, the dominant

features of the signal under analysis determine the type and order of the filter to be used for analysis. Some of the commonly used wavelets are as follows:

- **Haar:** It is one of the simplest types of wavelets. It is discontinuous and appears similar to a step function. It is the only orthogonal wavelet with a linear phase.
- **Daubechies:** The Daubechies wavelet family is named after its inventer, Ingrid Daubechies. It comprises a family of wavelets. Each wavelet in the family is represented using the notation dbN where 'N' represents the order of the wavelet. It is to be noted that the db1 wavelet is the same as the Haar wavelet.
- **Biorthogonal:** Biorthogonal wavelets have linear phase. Generally, these wavelets feature a pair of scaling functions and filters. One of the scaling functions in the pair is used for analysis and the other for synthesis. Different Biorthogonal wavelets are used for wavelet decomposition and reconstruction.
- **Coiflets:** Coiflets were, introduced by Daubechies at the request of R. Coifman. The Coiflet wavelet and scaling functions, have $2N$ and respectively $2N-1$ moments equal to zero.
- **Symlets:** These wavelets are very similar to the Daubechies wavelets and were indeed introduced as a modification of the Daubechies wavelets by Daubechies herself. Hence, both the Daubechies and Symlets wavelet families have very similar properties. Symlets are known for their nearly symmetrical functions.
- **Mexican Hat:** The Mexican Hat wavelet (or the Ricker wavelet) is derived from a function which is proportional to the second derivative of the Gaussian Probability Density Function (PDF). It does not have any scaling function.
- **Morlet:** Like the Mexican Hat wavelet, a Morlet wavelet also does not have a scaling function. But unlike the Mexican Hat wavelet, which is implicit, the Morlet wavelet is explicit.
- **Meyer:** Both the scaling and wavelet functions associated with the Meyer wavelet are represented in the frequency domain.

Figure 3 shows examples of the different types of wavelets.

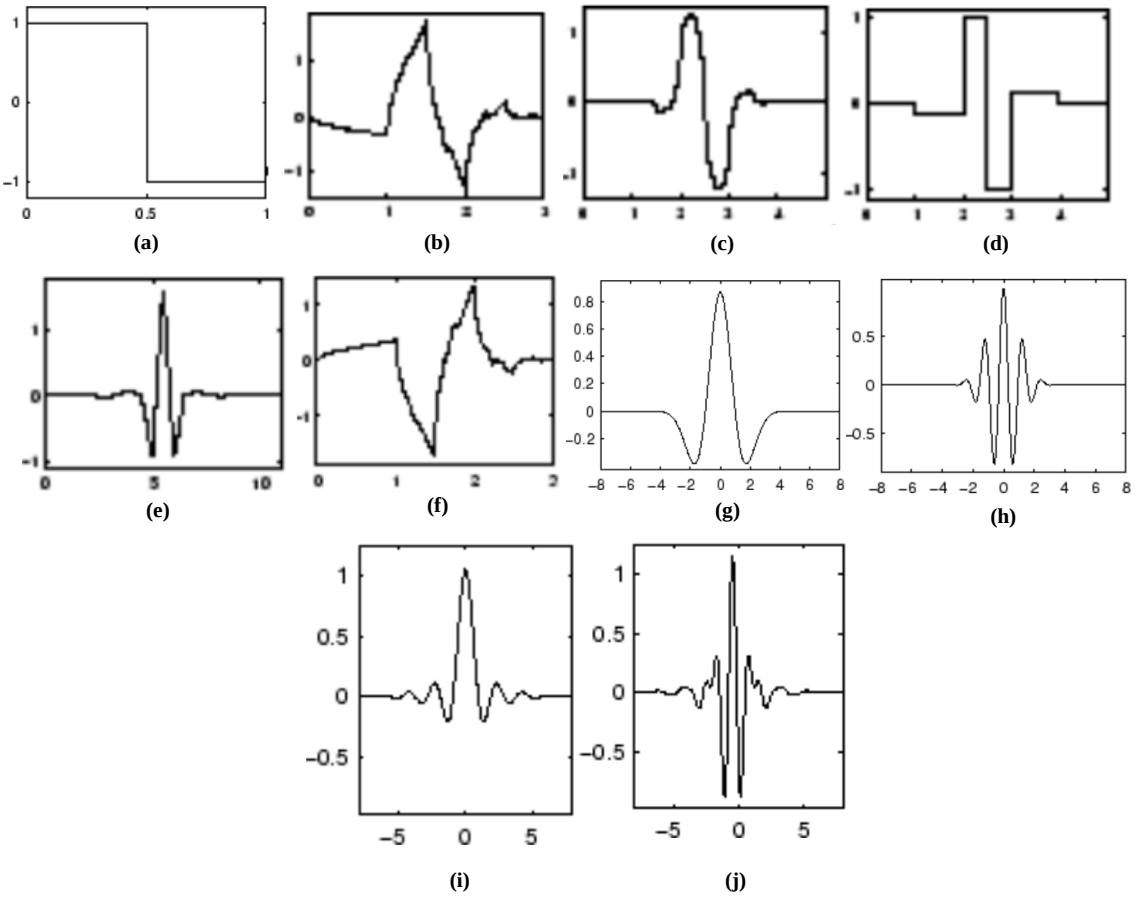


Figure 3 Different types of wavelets: (a) Haar, (b) Daubechies, db2, (c, d) Biorthogonal 1.3 pair, (e) Coiflet, coif2, (f) Symlet, sym2, (g) Mexigan hat, (h) Morlet, (i) Meyer scaling function, and (j) Meyer wavelet function.

From the point of view of signal processing, a wavelet is similar to a bandpass filter [29]. In particular, a wavelet transform can be considered as filtering using a set of octave band filters. When higher octave bands are added, more detail or resolution is added to the signal. Mallat [30], [31], and Meyer [32] introduced the concept of Multi-Resolution Analysis (MRA). They used MRA for constructing orthonormal bases of wavelets.

2.6.2.1 Implementation of Wavelet Transform using Filter Banks

The DWT is commonly implemented using filter banks. For example, a signal x[n] is simultaneously passed through a high pass filter with an impulse response h[n] and a low pass filter with an impulse response g[n]. The output of both the filters is subsampled by

a factor of 2. The output of the low pass filter g[n] after subsampling are called the approximation coefficients. On the other hand, the output of the high pass filter h[n] after subsampling, are called the detail coefficients (See Figure 4).

Figure 4 Block diagram of one level of discrete wavelet transform.

In order to further increase the frequency resolution, the sub-sampled output of the low pass filter is again passed through low and high pass filters. The new outputs are again sub-sampled i.e.,

$$y_{low}[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n-k]$$

$$y_{high}[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n-k]$$

Or more precisely,

$$y_{low} = (x * g) \downarrow 2$$

$$y_{high} = (x * h) \downarrow 2$$

where y_{low} and y_{high} are the outputs of the low pass and high pass filters respectively and $\downarrow$ represents a subsampling operation. This process can be represented with the help of a binary tree also known as a filter bank.

The process can be repeated several times, each time resulting in an increased frequency resolution. An example of a three-level filter bank is shown in Figure 5.

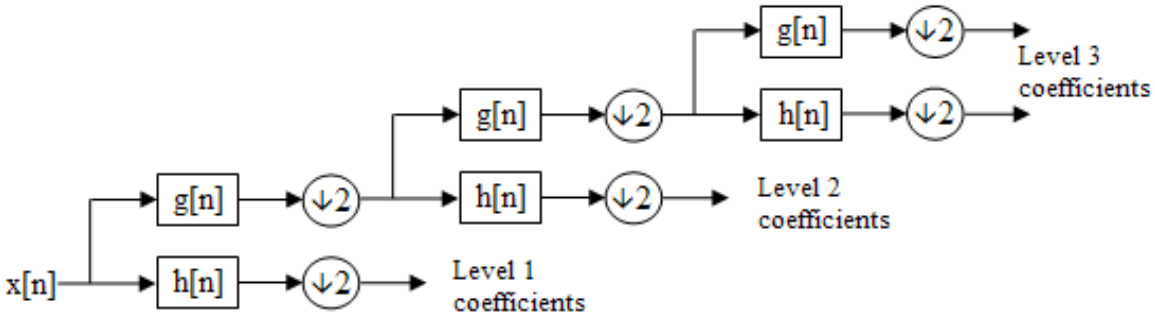


Figure 5 Example of a three-level filter bank.

At each level of the three-level filter bank shown in Figure 5, the signal is decomposed into low and high frequencies. The decomposition process requires the input signal to be a multiple of 2^n (n being the number of levels). An example of the frequency domain representation of the DWT is shown in Figure 6. Here, f_n represents the maximum frequency.

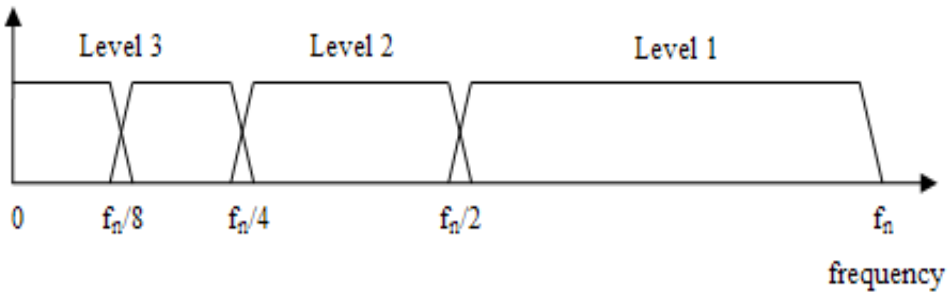
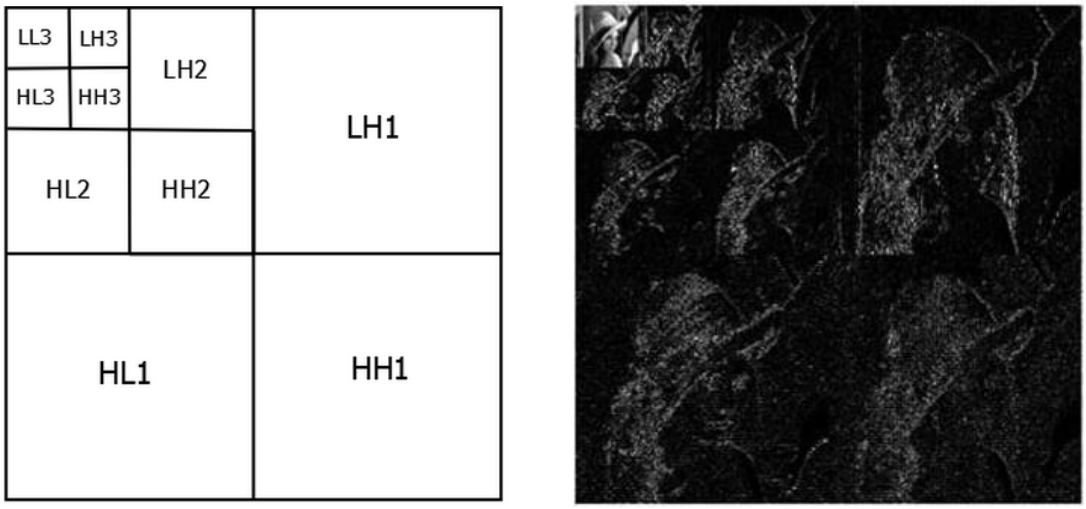


Figure 6 Frequency domain representation of 3-level DWT decomposition.

2.6.2.2 2D-Discrete Wavelet Transform

Since digital images are 2D signals, a two-dimensional DWT (2D-DWT) is required to analyse them. When a 2D-DWT is applied on an image, it splits the image into sub-bands of different frequencies as shown in Figure 7, where HH, HL, LH, and LL denote the High-High, High-Low, Low-High, and Low-Low sub-bands of the image, while the number following each pair denotes the decomposition level. At each level, the LL sub-band corresponds to (low frequency) approximation coefficients while the HL, LH, and

HH sub-bands correspond to (high frequency) detailed coefficients in vertical, horizontal, and diagonal directions respectively.



(a) **(b)**

Figure 7 Level 3 image decomposition using 2-D wavelet transform: (a) sub-band representation and (b) decomposition of Lena test image.

It is to be noted that the wavelet transform uses less coefficients to analyse low frequency content which has little variation (and as such there is no need to use too many coefficients to accurately describe it), while using more coefficients for the high frequency areas of an image, where the signal changes more often and therefore where more coefficients are required in order to accurately describe the signal (e.g., in Figure 7, the LL3 sub-band (which represents low frequency content) is much smaller than the HH1 sub-band (which represents the high frequency content).)

2.6.2.3 Advantages and Disadvantages of DCT and DWT

Some of the advantages and disadvantages of DCT and DWT are summarized below:

- ***Flexibility:*** DWT is more flexible compared to DCT. It is applied over the whole image unlike DCT which is applied over 8x8 pixel size blocks. While the DCT function is fixed, the DWT function is flexible and due to its multiresolution nature, it adapts better to the nature of the source data compared to the DCT.
- ***Compression Performance:*** DWT provides better energy compaction compared to DCT, leading to better compression performance. Typically, DCT provides

compression ratios of around 64:1 while DWT provides compression ratios of around 500:1 [33].

- ***Compression Artefacts:*** Since DCT is applied on small blocks, it introduces blocking artefacts in the compressed image. This is not the case with the DWT which is applied over the whole image. On the other hand, at higher compression ratios blurring and ringing artefacts are associated with DWT, although in general these tend to be better tolerated by the HVS than DCT blocking artefacts.
- ***Availability of HVS Models:*** Typically, better and/or more detailed HVS models exist for the DCT than for the DWT, not least because the DWT is a newer transform. On the other hand, the DWT structure and approach resembles a lot more how the HVS works, which in the longer term provides opportunities that the DCT cannot match.
- ***Adoption by Image Compression Standards:*** DCT is used in JPEG image compression standard while DWT is used in the more recent JPEG2000 image compression standard.

2.6.3 Discrete Multi-Wavelet Transform

The multiwavelet is a generalization of the idea of scalar wavelets. Unlike the conventional wavelets which use a single scaling function $(\emptyset(t))$ and a single wavelet $(\psi(t))$ function, multiwavelets use multiple scaling functions and wavelets. Generally, multiwavelet transforms can have r different scaling and wavelet functions. Multiwavelets with $r = 2$ have been used more commonly [101]. Mathematically, for the case of $r = 2$, the scaling and wavelet functions can be represented as:

$$\boldsymbol{\Phi}(t) = [\emptyset_1(t) \quad \emptyset_2(t)]^T \tag{7}$$

$$\boldsymbol{\Psi}(t) = [\psi_1(t) \quad \psi_2(t)]^T$$

where $\boldsymbol{\Phi}(t)$ and $\boldsymbol{\Psi}(t)$ are the multiscaling and multiwavelet functions respectively. For scalar wavelets, the following conditions have to be met:

$$\boldsymbol{\Phi}(t) = \sqrt{2}\sum_{k=-\infty}^{\infty} H_k \boldsymbol{\Phi}(2t-k) \tag{8}$$

$$\boldsymbol{\Psi}(t) = \sqrt{2} \sum_{k=-\infty}^{\infty} G_k \boldsymbol{\Psi}(2t - k)$$

where, for multiwavelets, both H_k and G_k are $2x2$ size matrices of filters. Mathematically, these quantities can be described as:

$$H_k = \begin{bmatrix} h_0(2k) & h_0(2k+1) \\ h_1(2k) & h_1(2k+1) \end{bmatrix} \tag{9}$$

$$G_k = \begin{bmatrix} g_0(2k) & g_0(2k+1) \\ g_1(2k) & g_1(2k+1) \end{bmatrix}$$

where, the matrices $h_k(n)$ and $g_k(n)$ represent the scaling and wavelet filter sequences and, for $k = 1, 2$, they meet the following conditions:

$$\sum_n h_k^2(n) = 1,$$

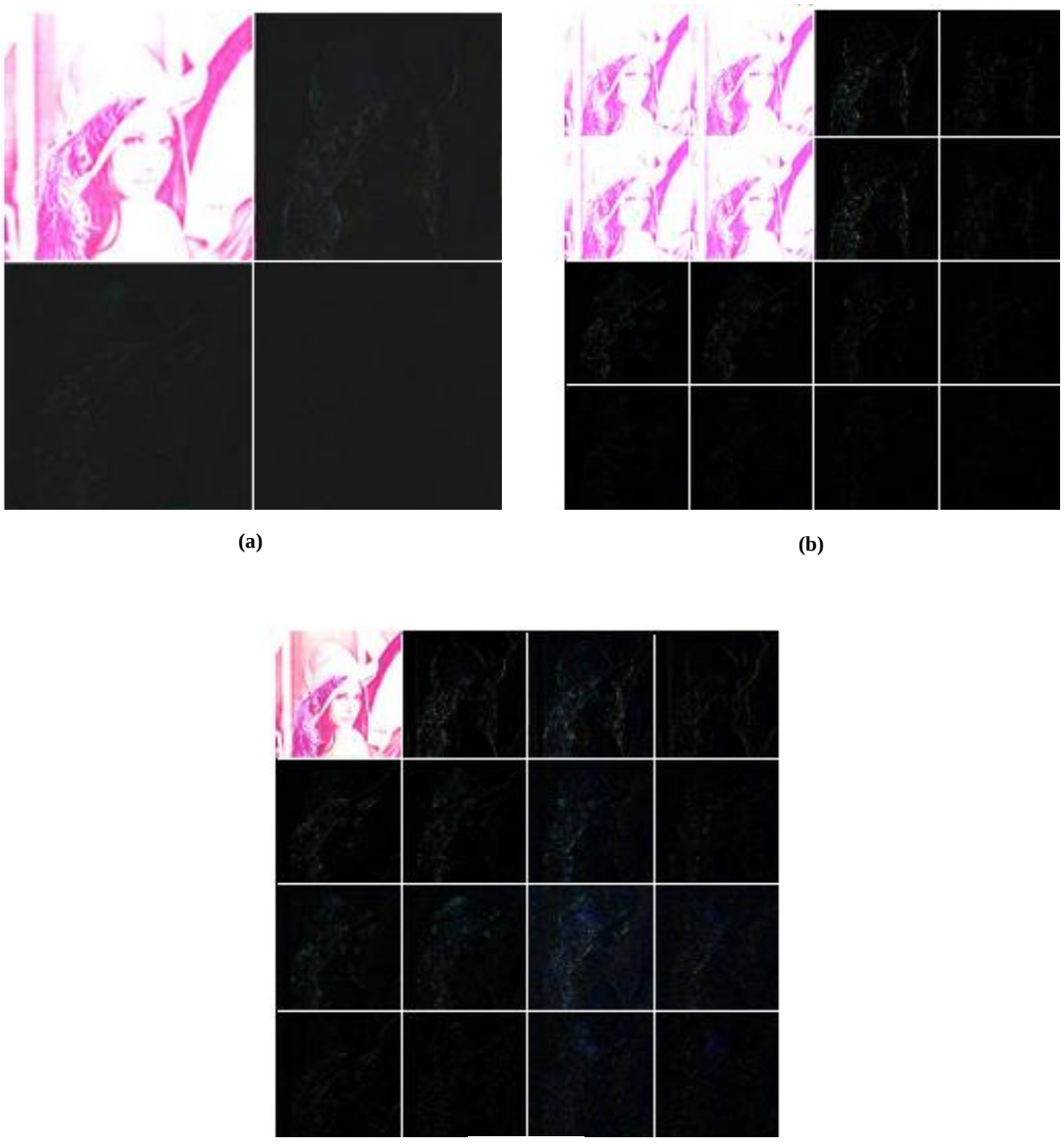
$$\sum_n g_k^2(n) = 1$$

The availability of more than one scaling and wavelet functions, allow multiwavelets to provide a higher degree of freedom in constructing the wavelets [96] and to overcome some of the scalar wavelet limitations. For example, unlike conventional wavelets, multiwavelets can simultaneously possess several desirable properties at the same time (e.g., orthogonality, symmetry, vanishing moments and compact support) [98] [99] [102].

Multiwavelets can be either balanced or unbalanced. The balancing of a multiwavelet is indicative of its energy compaction property. Unbalanced multiwavelets require 'pre-filtering' of the inputs while balanced multiwavelets do not require a pre-filter. This is because balanced multiwavelets possess preservation property [97] while unbalanced multiwavelets do not. Hence, balanced multiwavelets are generally more computationally efficient compared to unbalanced multiwavelets [97]. Figure 8 shows a visual comparison of the resulting sub-bands for the Antonini 9/7 scalar wavelet, the BAT01

balanced multiwavelet, and the GHM unbalanced multiwavelet applied to the Lena image.

It can be seen from Figure 8 that for each sub-band that the scalar wavelet creates, multiwavelets create four sub-bands. Moreover, the spectral content of the balanced multiwavelet is similar to that of the original image while that of the unbalanced multiwavelet is different [100].



(a) **(b)** **(c)**

Figure 8 One level decomposition of the Lena image using: (a) Antonini 9/7 wavelet transform, (b) balanced BAT01 multiwavelet transform, and (c) unbalanced GHM multiwavelet transform [100].

Similar to the wavelet transform, multiwavelet transform can also be implemented using filter banks. An example of a perfect reconstruction orthogonal multiwavelet filter bank ($r = 2$) is shown in Figure 9.

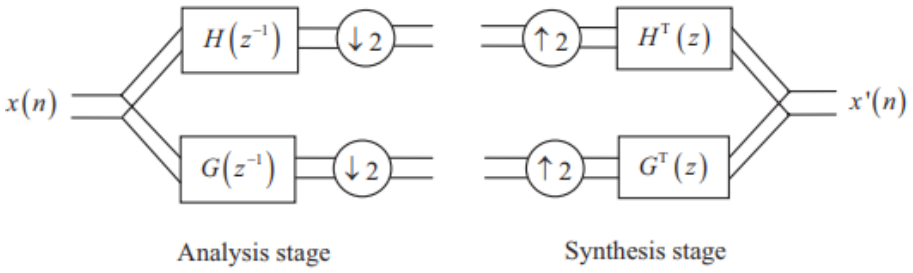


Figure 9 Perfect reconstruction orthogonal multiwavelet filter bank for ($\boldsymbol{r = 2}$) [101].

The filter bank in Equation (9) can also be transformed into a multi-channel, time-varying filter bank using the following equations:

$$\begin{bmatrix} H_0(z) \\ H_1(z) \end{bmatrix} = H(z^2) \begin{bmatrix} 1 \\ z^{-1} \end{bmatrix} \tag{10}$$

$$\begin{bmatrix} G_0(z) \\ G_1(z) \end{bmatrix} = G(z^2) \begin{bmatrix} 1 \\ z^{-1} \end{bmatrix}$$

where $H_0(z)$ and $H_1(z)$ are the transfer functions of two low-pass filters h_0 and h_1 respectively and $G_0(z)$ and $G_1(z)$ are the transfer functions of the two high-pass filters g_0 and g_1 respectively. This case is shown in Figure 10.

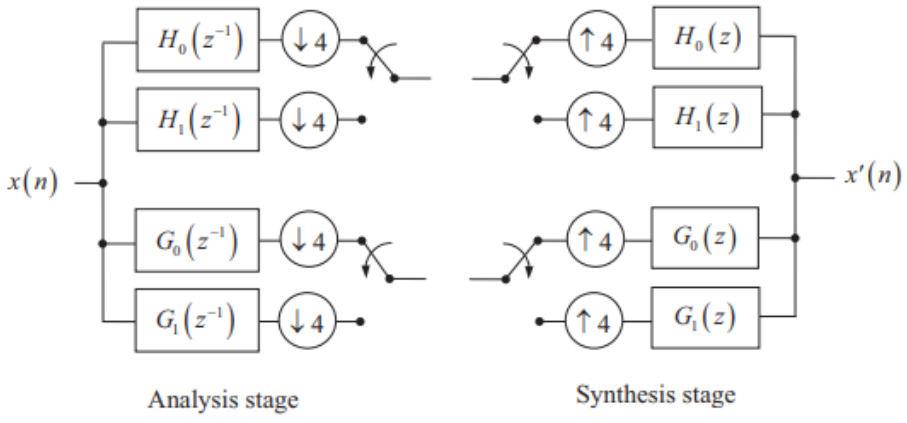


Figure 10 Time varying multiwavelet filter bank ($\boldsymbol{r = 2}$) [101].

CHAPTER 3: LITERATURE REVIEW

This chapter presents a review of the frequently used watermarking schemes from the literature. In order to better understand the schemes, they have been divided into two broad categories of spatial domain and transform domain techniques. Since the watermarking method proposed in this thesis is spread-spectrum based, a review of the frequently used spread spectrum based watermarking techniques is provided in Section 3.1. This is followed by a review of the spatial domain techniques in Section 3.2 and of the transform domain techniques in Section 3.3. Finally, the key differences between existing spread spectrum techniques and the proposed technique presented in this thesis and the novelty of the proposed technique are highlighted in sections 3.3 and respectively 3.4 of this chapter.

3.1 Spread-spectrum Watermarking Techniques

Spread spectrum techniques are frequently used in watermarking. The motivation behind spread spectrum communications is to deal with the conflicting fidelity and robustness requirements [34], [35], [36]. In spread spectrum communications a narrowband signal is spread over a much wider range of frequencies in such a way that the Signal-to-Noise Ratio (SNR) corresponding to any single frequency is very low. If the receiver has knowledge of the spreading function, it can use it to extract the transmitted signal to add up the signals in each of the frequencies such that the detector SNR is strong.

This characteristic of the spread spectrum techniques makes it possible to embed and detect weak watermark signals. Another advantage of the spread spectrum techniques is that it is difficult for an adversary to detect or jam a spread spectrum signal.

A drawback of the spread spectrum techniques is that they are very sensitive to desynchronization attacks, so countermeasures need to be employed to overcome this.

In the literature, spread spectrum techniques have been employed in both spatial and transform domains. These techniques are reviewed below.

Hartung et al. [9] propose modifications for common spatial-domain watermark embedding and extraction to avoid or counter a variety of attacks. The main idea is to adapt the power spectrum of the watermark to the host signal's power spectrum, and to employ an intelligent watermark detector with a block-wise multi-dimensional sliding correlator, which can recover the watermark even in the presence of geometric attacks. This technique is limited to spatial domain methods.

A spatial domain perceptual watermarking scheme based on the spread spectrum technique was proposed by Shyndel et al. in [37]. The technique is robust to small distortions in the watermarked image and allows for the insertion of multiple watermarks. However, the technique is not robust to more sophisticated attacks [38].

Cox et al. [7], [8] propose a DCT/FFT based watermarking scheme for grayscale images. The main idea here is that the watermark should be inserted into the perceptually significant regions of the image. This technique is limited to DCT/FFT and does not address the issue of watermarking in the wavelet domain which offers several advantages over both FFT and DCT as discussed in Chapter 2. Moreover, this is a non-blind method which will require the availability of the original image at the receiver which may not always be possible.

Perez-Friere et al. [12] compare the performance of spread-spectrum and quantization index based watermark embedding in images. They conclude that if the parameters of the quantization index based watermarking schemes are optimally selected, it may outperform the classical spread-spectrum based watermarking schemes under Additive White Gaussian Noise (AWGN) attacks i.e., an optimal selection of parameters for the quantization index based watermark embedding and under a low Watermark-to-Noise Ratio (WNR), the quantization based approach never performs worse than the spread-spectrum approach in terms of the achievable rate and probability of error. The main limitation of this technique is that the full spectrum of attacks has not been considered here. An AWGN attack is only one of the many possible types of attacks, and is generally perceived a mild form of an attack, and for a watermarking scheme to be useful, it is

important that it is robust to a variety of attacks and not just a single type of attack. Hence the conclusions drawn in this paper cannot be generalized for all types of attacks.

O'Ruanaidh et al. [82] describe how Fourier-Mellin transform (FMT) based invariants can be used for digital image watermarking. The embedded watermarks are designed to be unaffected by any combination of rotation, scale and translation transformations. The original image is not required for extracting the embedded watermark and hence the proposed method is an example of a blind watermarking scheme. The main limitation of this technique is that embedding in the FMT domain has several drawbacks e.g., it is computationally complex and in FMT, there is a need to maintain Fast Fourier Transform (FFT) symmetry, which halves the watermark capacity [83]. Moreover, this scheme considers a variety of attacks but, as it is shown later in this thesis, wavelets and multiwavelets can be used far more effectively and offer a higher capacity compared to Fourier transforms. Thus, among other limitations, this scheme provides a lower watermarking capacity than can be offered by a wavelet/multiwavelet based scheme.

Kutter et al. [84] present a perceptual model for embedding a watermark in an image. The embedding is performed using a spread-spectrum approach. The proposed model is based on the sensitivity and masking behaviour of the human visual system. The proposed scheme evaluates two different approaches for watermark insertion: inserting the watermark in the luminance components and inserting the watermark in the blue chrominance component. It concludes that compared to the luminance component, the blue component can accommodate a watermark of a much higher energy.
One of the main limitations of this approach is that it is a simple 1-bit watermarking scheme where a 1 denotes the presence of a watermark while 0 denotes its absence. It doesn't deal with multiple bits.

3.2 Spatial Domain Techniques

One of the earliest spatial domain blind watermarking techniques was proposed by Nikolaidis and Pitas [39]. This technique was based on slightly modifying the intensity of randomly selected image pixels. Their detection algorithm involves comparing the mean intensity value of the marked pixels against that of the unmarked pixels. The watermark is made resistant to JPEG compression and low pass filtering by minimizing the energy content of the watermark at higher frequencies while taking into account the properties of human visual system. A drawback of this scheme is that it assumes the presence of large areas of texture.

One of the simplest methods to embed a watermark in the spatial domain is to insert the watermark in the least significant bits (LSBs) of the pixels of an image [40]. An advantage of LSB based methods is that they are very simple to implement. Moreover, these methods are known to provide sufficient imperceptibility. On the other hand, a key drawback of these methods is that they generally have very poor robustness i.e., watermarks embedded using LSB methods are not only susceptible to common signal processing attacks, but it is also very easy to completely remove the entire watermark with little visual loss by simply resetting the LSB of each pixel.

Sharma and Sharma [41] also proposed modifying the LSB bits in their watermarking method. Their algorithm consists of the following steps: the first 2-bits of an 8-bit gray level image are replaced by the luminance part, the following 2-bits by the red component, the following 2-bits by green component and the last 2-bits by the blue component of the 32-bit image using a secret key. The advantage is that in this way the watermarking capacity can been increased and the resultant watermark will be unaffected by various attacks e.g. zero out LSB bits, cropping etc. The watermark is imperceptible in the resultant image.

Some more advanced spatial domain techniques are inspired from Genetic Algorithms (GA). For example, Wang et al.'s [42] multi-objective genetic algorithm based optimal image watermarking approach is designed to determine optimal watermarking parameters and embedding position.

Similarly, another genetic algorithm inspired method was proposed by Tsai et al. [43] to select the most adequate feature regions for robust image watermarking under the constraint of retaining the quality of the image. However, this method is very time consuming compared to other state-of-the-art methods.

Abraham and Paul [44] proposed a novel colour image watermarking scheme where the watermark is embedded in the host image using spatial domain techniques. The watermark is gradually spread over a certain region of the pixels. The technique has been shown to be efficient for a variety of geometric attacks. This method is simple and efficient but like all spatial domain techniques, its robustness against attacks is limited. Moreover, it does not take into consideration the HVS while embedding the watermark.

In general, while spatial domain techniques are simpler to implement, they are not as robust against attacks as the more complex transform domain techniques. Furthermore, spatial domain watermarking techniques also lack the benefit of relying on established HVS models developed in relation to various transform domain applications.

3.3 Transform Domain Techniques

Transform domain methods insert information into transform coefficients. Various types of transforms have been used for this purpose. The most common types of transforms used in the literature to date include: Fourier transforms [22] and fractional Fourier transforms [23], Cosine transforms [24], Wavelet transforms [25], fractional Wavelet transforms [26], and fractional Dual-Tree Complex Wavelet transforms, Multi-wavelet transforms, Hadamard transforms, Curvelet transforms and Singular Value Decomposition (SVD) transforms [27].

3.3.1 Fourier Transform Based Methods

Among the methods based on the Discrete Fourier Transform (DFT), Solichidis and Pitas [22] studied the statistical analysis of the behaviour of a blind robust watermarking system based on pseudorandom signals embedded in the magnitude of the Fourier transform of the host data.

They have calculated the distribution of DFT coefficients analytically, and found that the coefficient distribution is not exactly a Weibull distribution as earlier modelled by Cheng

& Huang [45]. They also showed that their proposed detector for multiplicative watermarks embedded in the DFT domain of non-white signals, outperformed a baseline correlator detector. Similarly, more recently, Cui [23] presented a dual digital watermarking embedding and detection algorithm which embeds a robust and a fragile watermark in the fractional Fourier transform domain of an image. The embedded watermark is perceptually invisible and robust to various image processing operations. However, since the method relies on the Fourier transform, it has a relatively high computational complexity. Another key Fourier transform based technique is O'Ruanaidh's Fourier-Melin transform based watermarking scheme described eralier in section 3.1 [82].

3.3.2 Discrete Cosine Transform Based Methods

Golestani et all.[46] introduced a logo watermarking method with unequal strengths based on DCT. This technique partitions the logo into smaller parts and inserts each part with unequal embedding strength. This technique is also called a 'layered' watermarking technique since it treats the logo as a combination of several 'layers' each of which is unequally important and thus requires unequal embedding strength. The results show that, when embedding binary logos into grayscale images, adopting the layered approach is superior to the more common single layer approach. However, it is not clear whether this method will be superior in the case of embedding in colour images. Moreover, the results show that this method performs very well in the case of simple logos but when the details in the logo this method may not perform as well as in the case of simple logos. In fact, its performance may be worse than that of the single layer approach. Hence, this method cannot be used for embedding logos with fine details.

Suhail et al. [24] embedded watermarks respectively in the DCT and DWT coefficients of an image and analysed the performance of this technique under JPEG and JPEG2000 compression in various conditions. They found that there were compatibility issues between the robustness of the watermarking algorithms and the two compression standards.

Yuliani and Rosiyadi [48] proposed a DCT based watermarking scheme which takes HVS into consideration while embedding the watermark. In this scheme, the watermark

is embedded into an image by modifying the DC coefficient values of the images. This method is robust against cropping and compression but its robustness against geometric attacks is not known.

DCT was also used in Wu et al.'s [47] proposed technique for robust watermarking. A binary watermark was used. The binary watermark is first scrambled with the motivation to achieve more security and robustness. Then, with the help of a Pseudo Random Number (PRN) and a secret key, a certain Alternating Current (AC) coefficient of the DCT is selected. Then, the average moment of the neighbouring coefficients around the selected AC coefficient is computed and the AC value is replaced by it. The watermarked image is obtained by taking the IDCT of the modified DCT coefficients. The application of this method is limited to grayscale images and it is not robust to translation attacks.

3.3.3 Wavelet Transform Based Methods

Chou and Liu [25] used the Discrete Wavelet Transform to embed a watermark in colour images in a way that satisfies two conflicting characteristics of a watermark i.e., transparency and robustness. Their proposed watermarking scheme enables creation of watermarks that are transparent and robust against various attacks such as cropping, low-pass filtering, scaling, median filtering, the addition of white noise, as well as JPEG and JPEG2000 compression at high compression ratios. The idea is to embed the watermark as perceptually redundant information. Hence, it is important to find distortion-tolerable host signals for watermark insertion. Equally important is to find the strength of the watermark that will make it imperceptible, yet robust. A drawback of this method is that it is not completely blind i.e., though it can work without requiring the original image to be present, it requires a small amount of information including the locations of qualified coefficients and the data associated with coefficient quantization for watermark extraction.

Fractional wavelet transform is a variant of the discrete wavelet transform. Based on encryption in the fractional discrete wavelet transform domain, Bhatnagar and Raman [26] proposed a robust watermarking scheme to improve the protection and authentication of images. They combined the two concepts of cryptography and watermarking and proposed a novel watermarking scheme based on encryption

techniques. The encryption is performed in the fractional wavelet transform domain. Their main idea is to perform encryption in the fractional wavelet transform domain and to embed the watermark inside the encrypted image by modifying its singular values.

The maxima values of the wavelet transform, called Wavelet Transform Modulus Maxima (WTMM) [49], [50], provide interesting insights about an image. For example, they represent edges in an image and unlike the standard DWT which is not translation invariant, WTMM coefficients are translation invariant. This property of WTMM was exploited by Alghouniemy and Tewfik [51]. Their proposed method tries to correct geometric distortions in image watermarking i.e. the method estimates the scaling factor of a previously scaled watermarked image and the angle by which the image has been rotated. In particular, the method computes the Edges Standard Deviation Ratio (ESDR) to get an estimate of the scaling factor and the Average Edges Angles Difference (AEAD) to approximate the angle of rotation. Both ESDR and AEAD are computed from wavelet maxima locations. The proposed method does not require the original image if the image has been normalized before transmission. The idea is that since wavelet transform maxima represents edges in an image, if an image is scaled by a factor γ, then its wavelet maxima should also be scaled by the same factor. Similarly, if an image is rotated by an angle θ, then its wavelet maxima should also be rotated by a similar angle. This assertion can be used to estimate γ and θ by comparing standard deviation and angles of wavelet maxima locations respectively from a reference point (called Maxima Location Mean (MLM) in this case) before and after scaling/rotation. A problem with this method is that its effectiveness has been shown using only a limited range of attack parameters. Moreover, the method requires prior information about the original image, even though it does not rely on the presence of the original image during detection.

WTMM was also used by Luo, Xing, and Shi [52]. In [52] mutual information was used to detect the presence or absence of the watermark. Moreover, it only targeted watermarking of grayscale images.

Elijah Mwangi [53] proposed a DWT based geometric attacks invariant method which exploits the properties of centroids of an image to calculate parameters of RST distortions. A drawback of this method is that it requires the system to be informed about

which one of the RST distortions (rotation, scaling, and translation) has occurred, to calculate correct parameters.

Senthil & Bhaskaran [54] proposed another simple DWT based RST invariant watermarking scheme which embeds the watermark in the 3rd level approximation (LL) sub-band coefficients of DWT. They use the Daubechies family of wavelets. The main drawback of this method is that it is too simple to practically save against a variety of attacks.

Patvardhan, Kumar, and Lakshmi [56] proposed a DWT based robust watermarking scheme for colour images (YCbCr). In this method, first the watermark text is converted into a Quick Response (QR) code. It then uses the diagonal sub-band (HH) of the DWT to embed the watermark. The results show that the method is robust against Salt & Pepper noise and JPEG compression but its robustness against RST attacks is very weak. Moreover, this method does not take the HVS into consideration.

Hu, Shao, and Ma [57] exploit the human visual system and the DWT in their proposed watermarking scheme. They first scramble the watermark using a logistic map. The scrambled watermark is then embedded into the DWT coefficients. To improve the robustness and transparency of the watermark, the authors expand the contrast sensitivity function (CSF) to the spatial frequency plane to determine the perceptual weight of the embedding strength in the DWT sub-bands. The experimental results show that the proposed method not only results in a high quality watermarked image but is also resistant to compression, filtering, noise (Gaussian and Salt & Pepper), enhancement, and geometric attacks. However, the results have only been demonstrated using a grayscale host image and a binary watermarked image. It is not clear how well the algorithm will perform in the case of colour images.

3.3.4 Singular Value Decomposition Based Methods

Singular Value Decomposition (SVD) is another common technique which has been often used in watermarking. The properties that make SVD particularly useful for watermarking, are that singular values are unique for a given matrix and that the singular values of an image have very good stability i.e., when a slight change happens in an image matrix, its singular values do not change considerably. Typical examples of using

SVD for watermarking are illustrated by Liu et al. [27] and by Chandra [58]. Liu added the watermark to the coefficients obtained after applying SVD on the host image. On the other hand, Chandra embedded the SVD coefficients of the watermark in the SVD coefficients of the host image.

However, the use of SVD transform for watermarking has two major drawbacks. One, is that the resultant watermarked image is not robust against common attacks, and the second is that it results in quality degradation of the host image. That is why more sophisticated watermarking schemes use SVD in combination with either the DCT or DWT [59].

3.3.5 Other Transforms

The Arnold Transform [60] is another transform which has been used in watermarking techniques. Its advantage in the context of watermarking is that it provides good security and is simple to compute [61]. For example, the Arnold transform of an image $I(x,y), x, y \in \{0,1,2,\dots,N-1\}$ is basically a transformation of the point (x,y) into another point (x', y'), where $x' = (x+y)\ mod\ N$ and $y' = (x+2y) mod\ N$.

The use of Arnold transform in watermarking was proposed by Naseem et al. who proposed a robust blind watermarking method for medical images [61] that is resistant to geometric attacks. In the proposed method, the image is encrypted twice: first, when the watermark is embedded chaotically, and second, when the watermarked image is scrambled before transmitting. For robustness, the proposed method relies on statistical moment normalization techniques, i.e. the original image is firstly made invariant to geometric attacks, then the watermark is embedded chaotically in the feature space of the image which is moment normalized. The main limitation of this method is that its application is limited to medical images which are generally uncompressed images. Since non-medical images are generally compressed before storage or transmission, the proposed method might not be suitable there.

Wang et al. [90] used the Polar Harmonic Transform (PHT) [62] and Non-Subsampled Shearlet Transform (NSST) [63] to address the issue of robustness in watermarking. The application of this method is limited to grayscale images only. Similarly, Zhang & Meng [64] used a Contourlet Transform and QR code based robust image watermarking

scheme. This technique suffers from the inherent limitations of the QR code. Moreover, the effectiveness of the proposed technique is not clearly demonstrated.

To deal with the problem of scaling attacks on watermarked images, Zhang, Wang, and Zhou [65] proposed to use the Scale Invariant Feature Transform (SIFT) in addition to using DWT and SVD for watermark embedding. This method is affected by the inherent false positive problem associated with SVD. Moreover, if a false singular value matrix is provided, the scheme cannot differentiate between a false and a true singular value matrix. Moreover, the application of this method is limited to grayscale images.

3.3.6 Combination of Various Transforms

Ma, Zhang, and Li [66] found that DWT, Walsh Transform, and SVD can be combined to provide robustness against RST attacks, as well as cutting and tampering (overwriting) attacks, i.e. even if a part of the image is cut, or if part of the image has been over-written, the watermark can still be recovered. The main drawback of this algorithm is that it has only been applied to grayscale images and its performance for coloured images is still unknown. Moreover, the algorithm does not clearly explain how the combination of DWT, Walsh Transform, and SVD helps in robustness.

Khalili [67] combined Arnold Transforms (AT) with DCT to develop a robust watermarking scheme for colour images. In this scheme, the watermark is scrambled using the Arnold transform, while the scrambled watermark is embedded in the middle frequencies of the DCT coefficients. This method works well against rotation, compression, and salt & pepper noise but it is not robust against scaling and translation attacks. Hence, overall, with the exception of rotation, this method does not provide robustness against geometric attacks.

Makbol et al. [55] combined DWT and SVD to develop a robust watermarking scheme for grayscale images. In this scheme, the watermark is embedded into the LL sub-band of the DWT. It targets geometric attacks (rotation, scaling, and translation) as well as compression and salt & pepper attacks but its performance against geometric attacks is very weak. Moreover, it cannot be applied to colour images directly. Ansari & Pant [68] also combined DWT and SVD in their proposed robust watermarking scheme. In this method, first the host image is transformed using DWT. Then, the singular values of the

transformed host image are modified using the principal components of the watermark. Once the watermark is inserted, the last two LSBs of the host image are modified.

This modification includes insertion of the scrambled and deterministic average representation of the host image along with the SVD based tamper identification information. These LSBs can be used to identify the tampered region. Moreover, in this method, the Artificial Bee Colony (ABC) [69] scheme is used as a further optimization technique. A drawback of this algorithm is that it has been designed to target only grayscale images. Its application to colour images may not be equally efficient.

Another DWT and SVD based technique was proposed by Rasti, Anbarjafari, and Demirel [70]. This method used a QR code which has an inherent drawback that if the embedding algorithm is known, then a QR code scanner software can be used to easily extract the watermark. Moreover, the proposed algorithm has shown to be efficient only in the case of a scaling attack. Its performance under other geometric attacks (such as rotation and translation) is not known.

Similarly, Jia, Zhou, and Zhou [71] and Su et al. [72] also proposed QR code and DWT based algorithms which are also affected by QR codes' inherent limitations. Moreover, the performance of Jia, Zhou, and Zhou's method [71] under rotation and translation is not known.

Jane, Elbasi, and Ilk [73] also proposed a DWT and SVD based robust watermarking scheme but only showed its effectiveness for a limited set of rotation and scaling factor values which limits its application in more general cases.

Rajput & Tiwari [74] proposed to combine DWT and DCT for robust watermarking of RGB colour images. A problem with this method is that it is only robust against blurring attack. It is not designed to be robust against geometric attacks. Hence, its application is rather limited. Moreover, although this method is aimed at RGB colour images, it does not take the HVS into consideration.

Lin, Niu, and Jiang [75] also proposed a robust watermarking scheme which combined DCT and DWT. In this method, first feature points are extracted using the Harris detector [76]. This results in the development of a feature point set. This is then followed by a step in which the geometric parameters are calculated with the help of set matching using

the Hausdorf distance [78]. Lastly, DWT is applied using the Harris feature points as centre. The Low-Low (LL) sub-band of the DWT is further transformed using DCT.

The watermark is embedded in the obtained DCT coefficients. This method is computationally complex. Moreover, it only targets grayscale images and it may not perform equally well in the case of colour images. Another problem with this method is that it targets only scaling and rotation correction but it cannot be used in the case of translation attacks.

Saravanan et al. [79] proposed to combine DWT, DFT, DCT, and SVD for efficient and robust watermarking of colour images. In this method, the Daubechies family of wavelets is used. The DWT stage uses the horizontal detail coefficients for watermark embedding. Since DWT is not translation invariant, DFT is used to compensate for that. This is followed by DCT, which allows a compact representation of the information. Finally, SVD is used to embed the watermark in the image. The drawbacks of this algorithm are that it is not scale invariant, it is computationally complex, and it has low capacity.

DWT, DCT, and SVD were also combined in Fazli & Moeini's [80] robust image watermarking scheme. In this scheme, the host image is first divided into four non-overlapping rectangular regions called sub-images. A copy of the watermark is embedded into each sub-image. This distribution of the watermark into different parts of the image is expected to protect from cropping of parts of the image. For robustness against geometric attacks, a synchronization scheme is used which detects the image corners of the desired image. This method is robust against a variety of attacks and works for colour images, but it does not take into consideration HVS while embedding the watermark. Hence, its capacity can be further improved.

Kumar et al. [81] combined DWT with rough set theorem and SVD for efficient watermarking of grayscale images. SVD was used to make the watermarking scheme robust, while rough set theorem was used to enhance the perceptual quality of the watermark. The problem with this method is that its robustness to rotation is limited. Moreover, this method only addresses the problem of watermarking of grayscale images and it is computationally complex. As a general conclusion, transform domain methods have been found to be more robust to attacks compared to spatial domain methods [1].

Furthermore, the availability of HVS models for some transforms makes their use more appealing to watermarking, as HVS-based embedding leads to increased robustness and decreased watermark visibility.

3.4 Differences Between the Existing Techniques and the Proposed Technique

The main differences between the existing and the proposed technique are:

- The proposed technique is based on watermark embedding in the RGB colour domain.
- The proposed technique embeds a logo as a watermark rather than some generic binary data. For example, in the case of logo, the watermark can be inspected visually and the error correction ability of the HVS is used to decide the presence or absence of the watermark. Hence, it is no longer required that the recovered watermark be an exact copy of the embedded watermark. Rather, a certain amount of loss, which is not visually significant, can be tolerated. The HVS is essentially used as an error correction code. The embedding is done in all the RGB components (Red, Green, and Blue) where the strength of the watermark in each component is weighted by its importance to the HVS.
- The proposed technique also investigates and analyses the use of Wavelet Transform Modulus Maxima (WTMM) as a way of improving robustness to geometrical attacks. The use of WTMM has been little investigated so far in the context of watermarking.
- The proposed technique embeds two different watermarks in the wavelet/multiwavelet domains. The two watermarks are embedded in different sub-bands, are orthogonal, and serve different purposes. One is a high capacity multi-bit watermark used to embed the logo, and the other is a 1-bit watermark which is used for the detection and reversal of geometrical attacks.

It is worth noting that although WTMM has been very little used in digital watermarking, it has been used quite extensively especially for image fusion in the field of medical imaging [86], [87] and for stereo correspondence matching in stereo vision applications, where it has shown very good promise.

Zhu and Zhu [85] is amongst the very few authors that employed WTMM in watermarking. In their method, the modulus maxima of the wavelet transform decomposition is used for watermark embedding. Their method basically combines this digital watermarking scheme with a digital signature algorithm to improve the safety of the digital signature, and is very different to the scheme proposed in this thesis.

3.5 The Novelty of the Proposed Technique

The main contributions of this thesis are the investigation into the use of WTMM for robust watermarking of color images and for improving watermark robustness to geometrical transformations.

The translation invariance property of the WTMM is particularly useful when fighting against geometrical attacks on watermarks. Furthermore, the use of WTMM is investigated for both wavelets and multiwavelets. This investigation adds a positive contribution to the existing body of knowledge in the field of digital watermarking. Another innovative feature of the proposed watermarking scheme is its particular use of dual watermarks i.e., the proposed scheme embeds two orthogonal watermarks in the wavelet and respectively the multiwavelet domains.

The proposed scheme also looks at how the HVS can be taken into account and adaptively used for RGB images. For example, the human eye has different levels of sensitivity for different colour components and different frequencies. This fact is exploited by embedding watermarks of different strengths in each color component according to the sensitivity level of the eye to a particular colour component. Same goes for different frequencies.

The proposed method covers the limitations of the existing techniques i.e.

1. It deals with RGB colour images, taking into account the characteristics of the HVS. By watermarking images in the RGB domain, the chip rate associated to a spread spectrum system is increased three-fold compared to watermarking grayscale images, which improves cross-correlation performance and watermark robustness.
2. It embeds an invisible logo making use of the native error correction capabilities of the HVS as an aid in dealing with watermark errors.
3. It is based on transforms that hold a lot of promise in the context of watermarking (wavelets and multiwavelets).
4. It takes advantage of the properties of the WTMM for watermarking purposes with the specific aim of countering a variety of geometric attacks (e.g., rotation, scaling, and translation).
5. It is more robust than, and shows good promise compared to, other state-of-the-art RGB watermarking methods.

CHAPTER 4: WAVELET TRANSFORM MODULUS MAXIMA

This chapter presents an introduction of the Wavelet Transform Modulus Maxima (WTMM). WTMM is one of the fundamental techniques that are being used in the scheme proposed in this thesis. Hence, an overview of the related concepts is presented in this chapter. In the first section, WTMM is introduced. The general procedure used for calculating the WTMM is presented in the second section, while the practical implementation of WTMM in MATLAB is covered in the third section of this chapter.

4.1 Wavelet Transform Modulus Maxima and its Applications

This section presents an introduction of WTMM. WTMM was first introduced by Mallat and Hwang in 1992 for the detection of singularities of a function [92]. Since then, it has been commonly used for edge detection (e.g., in medical ultrasound images [93]), for fusion of medical images [86][87], and for stereo correspondence matching in stereo vision applications [50]. It has also been used for characterizing and identifying the behaviour of heart signals as recorded on Electrocardiogram (ECG) [94][95]. Moreover, images can also be reconstructed from the modulus maxima values without any visual distortions [92]. Generally, WTMM has many advantages [92] but in this research, it has been used mainly because of its shift-invariance property. It is the WTMM's shift invariance property, which wavelets and multiwavelets do not have, that enables the proposed watermarking scheme to identify and undo geometrical attacks. In other words, the shift invariance property of the WTMM ensures that when an image is translated, the resulting WTMM values are also translated, but without being modified. In order to understand how WTMM is utilized in the proposed watermarking scheme, it is important to understand the underlying mathematical details of WTMM first.

Consider an image $F\ (x, y)$ and let $\theta\ (x, y)$ represent a 2D low pass filter. Let $\psi^1(x, y)$ and $\psi^2(x, y)$ represent two partial derivative functions of $\theta\ (x, y)$ along the horizontal and vertical directions respectively. The functions $\psi^1(x, y)$ and $\psi^2(x, y)$ are defined in Eq. (11) and Eq. (12) respectively [52][91] as:

$$\psi^1(x,y) = \frac{\partial\theta}{\partial x}(x,y) \tag{11}$$

$$\psi^2(x,y) = \frac{\partial\theta}{\partial y}(x,y) \tag{12}$$

Let s denote the scale of wavelet transform. Then, the partial derivatives of $\theta(x,y)$ at each scale can be defined as ${\psi^1}_s(x,y) = \left(\frac{1}{s}\right)^2 \psi^i\left(\frac{x}{s},\frac{y}{s}\right), for\ i = 1,2$. The wavelet transform $WF(s,x,y)$ at each scale s has two components $W^1F(s,x,y)$ and $W^2F(s,x,y)$. These components represent the horizontal and vertical directions of wavelet transform as denoted in Eq. (13).

$$\begin{pmatrix} W^1F(s,x,y) \\ W^2F(s,x,y) \end{pmatrix} = s\begin{pmatrix} F*{\psi^1}_s(x,y) \\ F*{\psi^2}_s(x,y) \end{pmatrix} \tag{13}$$

The magnitude ($Mf(s,x,y)$) and the angle ($Af(s,x,y)$) of the WTMM can be computed as:

$$Mf(s,x,y) = \sqrt{|W^1f(s,x,y)|^2 + |W^2f(s,x,y)|^2} \tag{14}$$

$$Af(s,x,y) = \begin{cases} \alpha(s,x,y), & if\ \ W^1f(s,x,y) \geq 0 \\ \pi + \alpha(s,x,y), & if\ \ W^1f(s,x,y) < 0 \end{cases} \tag{15}$$

where, $\alpha(s,x,y) = tan^{-1}\left(\frac{W^2f(s,x,y)}{W^1f(s,x,y)}\right)$.

The WTMM coefficients can be identified by applying a suitable threshold to the magnitude *Mf* of the WTMM and can be represented with the help of a binary image where white and black pixels correspond to zero and respectively large-amplitude (modulus maxima) coefficients. The angle *Af* of the WTMM represents the angles at the points where the modulus is nonzero.

4.2 General Procedure for Calculating the Wavelet Transform Modulus Maxima

The WTMM can be calculated using the following steps:

1. Separate the LH and HL parts of the wavelet transform coefficients so that they can be used to calculate the absolute value (magnitude) and angle of the WTMM.

2. Compute the magnitude (absolute value) of wavelet transform coefficients using Eq. (14).
3. Use a threshold value to retain the wavelet transform coefficients with a magnitude larger than the threshold value and discard the wavelet transform coefficients with a magnitude smaller than the threshold value.
4. Compute the angle of wavelet transform coefficients using Eq. (15).
    a. Quantize the angle to the multiple of $\left(\frac{\pi}{4}\right)$ to force the angle to start from 45 degrees.
    b. Obtain the quantized angle.

The procedure for quantization of the angle is as follows:

1. Round the angle (MATLAB's 'round' function can be used here) values to the nearest integer value.
2. Divide the rounded values by $\left(\frac{\pi}{4}\right)$.
3. The new values obtained after Step 2 are used as the direction of the angle. There are eight possible directions: 0 degree, 45 degrees, 90 degrees, 135 degrees, 180 degrees, 225 degrees, 270 degrees, and 315 degrees. These angles correspond to the horizontal (right), diagonal (right, up), vertical (up), diagonal (left, up), horizontal (left), diagonal (left, bottom), vertical (down), and diagonal (right, bottom) directions respectively.

(x-1,y+1)	(x,y+1)	(x+1,y+1)
(x-1,y)	(x,y)	(x+1,y)
(x-1,y-1)	(x,y-1)	(x+1,y-1)

Figure 11 The Central pixel and its eight neighbouring pixels which are used for calculating the Wavelet Transform Modulus Maxima directions.

The central pixel and its eight neighbouring pixels which are used for determining the direction are shown in Figure 11. The relevant direction is decided by the value of the angle.

4.3 Experimental Results of Wavelet Transform Modulus Maxima

This section presents experimental results obtained for WTMM. Figure 12 – Figure 14 show the vertical detail (LH) wavelet sub-bands, horizontal detail (HL) wavelet sub-bands, WTMM magnitude (*Mf*), WTMM angle (*Af*), and WTMM coefficients corresponding to the 1st level, 2nd level and 3rd level DWT decomposition respectively. The results are shown for four different images: Lena, Barbara, Airplane, and Pepper.

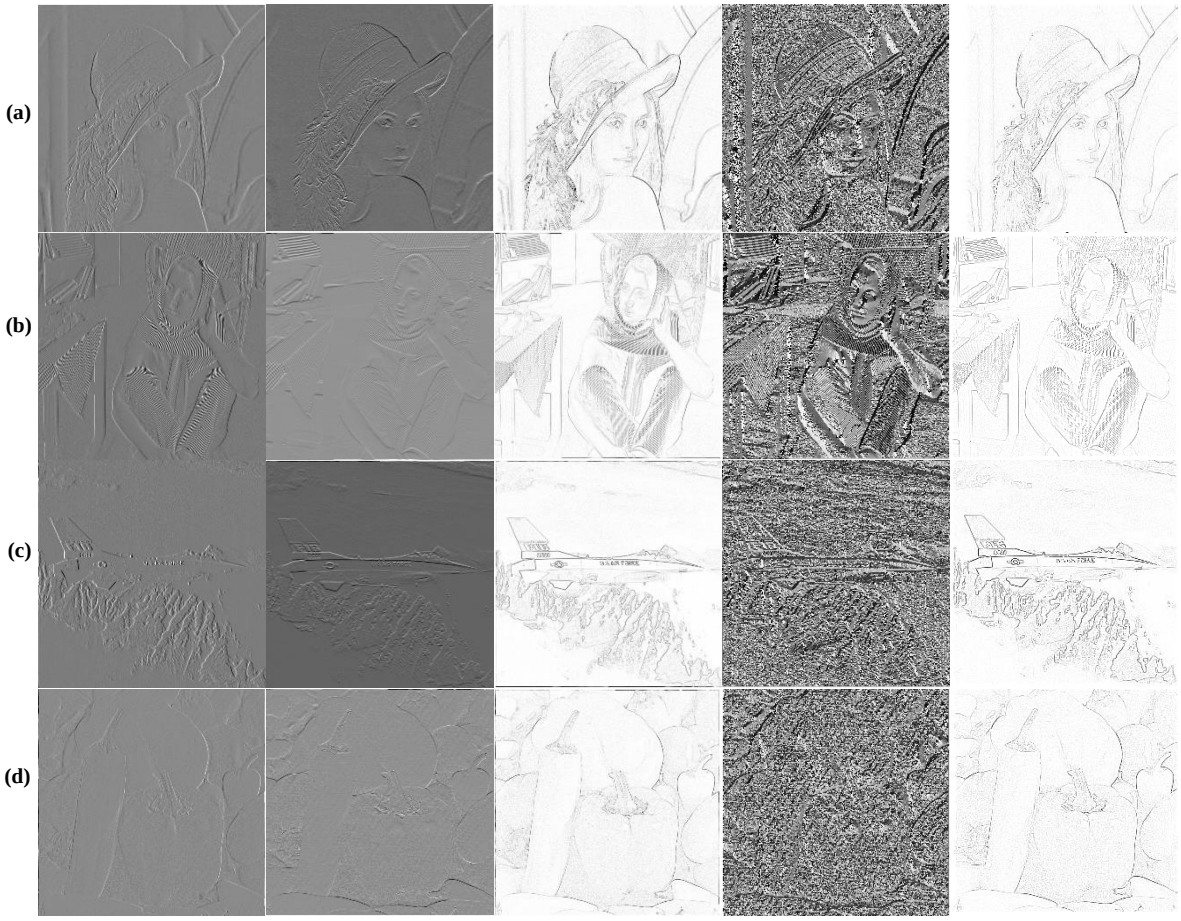


Figure 12 WTMM examples of 1st Level DWT for (a) Lena, (b) Barbara, (c) Airplane, and (d) Pepper images. From left to right: LH1wavelet sub-band, HL1 wavelet sub-band, WTMM magnitude (*Mf*), WTMM angle (*Af*), and WTMM coefficients.

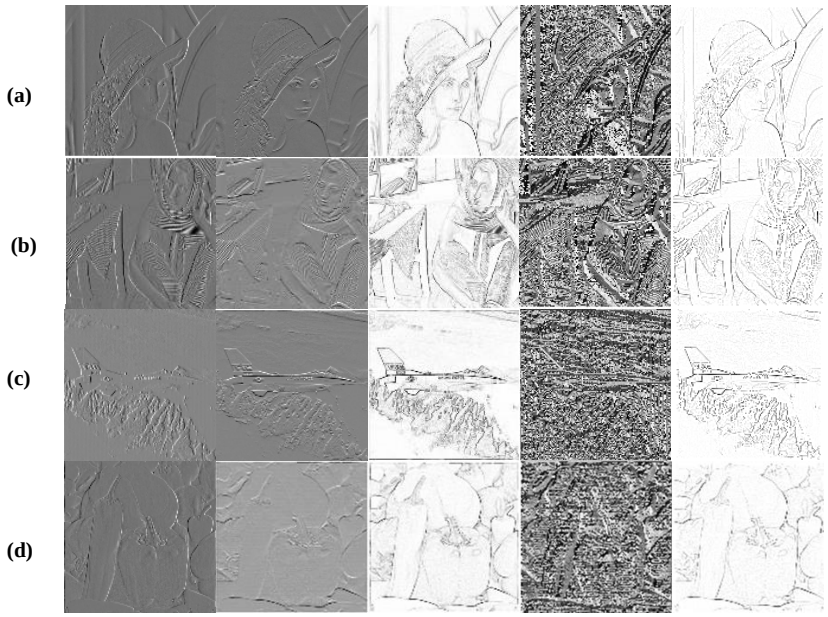


Figure 13 WTMM examples of 2nd Level DWT for (a) Lena, (b) Barbara, (c) Airplane, and (d) Pepper images. From left to right: LH2 wavelet sub-band, HL2 wavelet sub-band, WTMM magnitude (*Mf*), WTMM angle (*Af*), and WTMM coefficients.

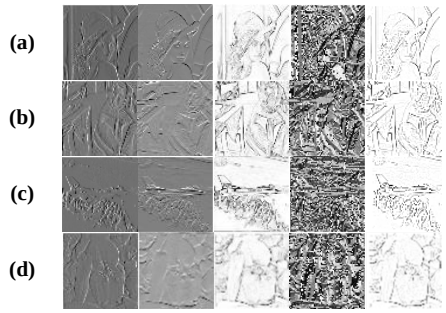
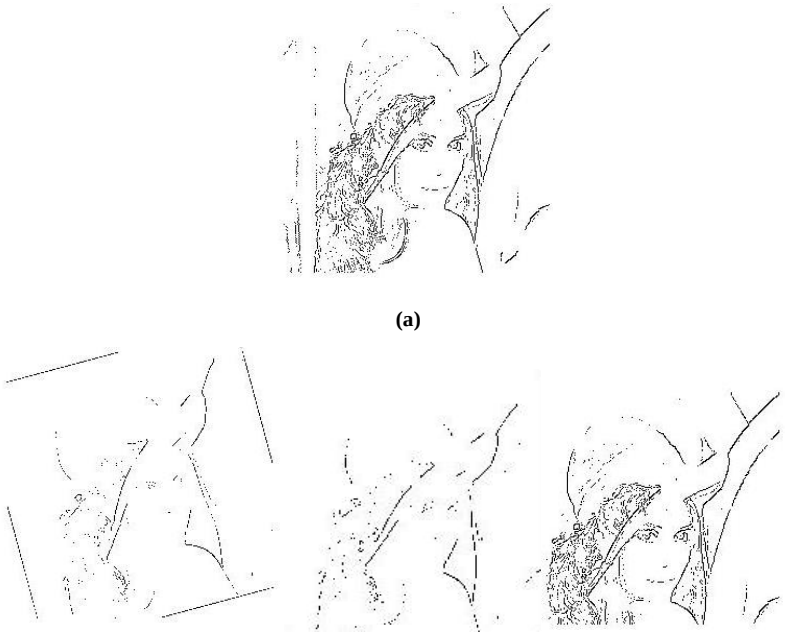


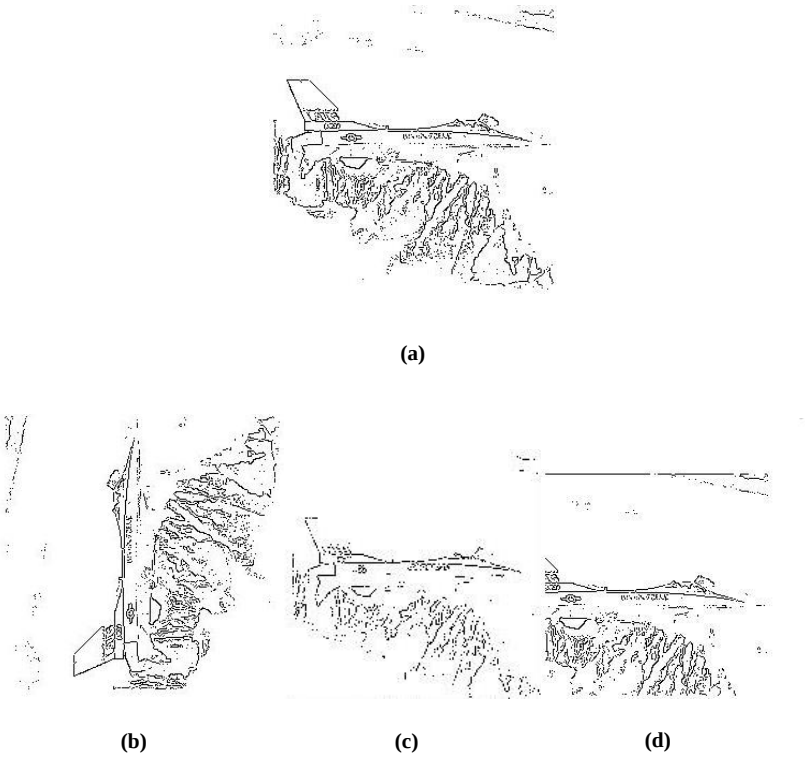
Figure 14 WTMM examples of 3rd Level DWT for (a) Lena, (b) Barbara, (c) Airplane, and (d) Pepper images. From left to right: LH3 wavelet sub-band, HL3 wavelet sub-band, WTMM magnitude (*Mf*), WTMM angle (*Af*), and WTMM coefficients.

Figure 15 – Figure 16 show some visual examples of the WTMM coefficients output for rotation, scaling and translation.



(a) **(b)** **(c)** **(d)**

Figure 15 (a) WTMM of the original Lena image; (b) Lena watermarked image rotated by (15^o); (c) Lena watermarked image scaled by (0.7); (d) Lena image watermarked translated by (80, 80).



(a) **(b)** **(c)** **(d)**

Figure 16(a) WTMM of the original Airplane image; (b) Airplane watermarked image rotated by (90^o); (c) Airplane watermarked image scaled by (0.7); (d) Airplane watermarked image translated by (96, 96).

CHAPTER 5: METHODOLOGY

This chapter presents a detailed description of the proposed robust logo image watermarking technique for colour images. The proposed technique consists of two parts: watermark embedding and watermark detection. Watermark detection itself is a two-stage process. The proposed watermark embedding technique is presented in Section 5.1 while the proposed watermark detection technique is presented in Section 5.2.

5.1 Watermark Embedding

The key features of the proposed watermark embedding technique are the embedding of two orthogonal watermarks in different DWT sub-bands of the same host image and the use of the shift invariant wavelet transform modulus maxima for achieving robustness against geometric attacks. The first watermark is a robust 1-bit watermark which is embedded in the Low-High (LH) and High-Low (HL) sub bands of the DWT of the original image, while the second watermark is a high capacity multi-bit watermark (a logo image) which is embedded in the High-High (HH) sub bands of the DMWT of the watermarked image already containing the 1-bit watermark. The 1-bit watermark is embedded in the wavelet domain, using the Haar wavelet, while the multibit watermark is embedded in the multiwavelet domain using the Cardbal2 multiwavelet. The proposed watermark embedding technique is shown in Figure 17.

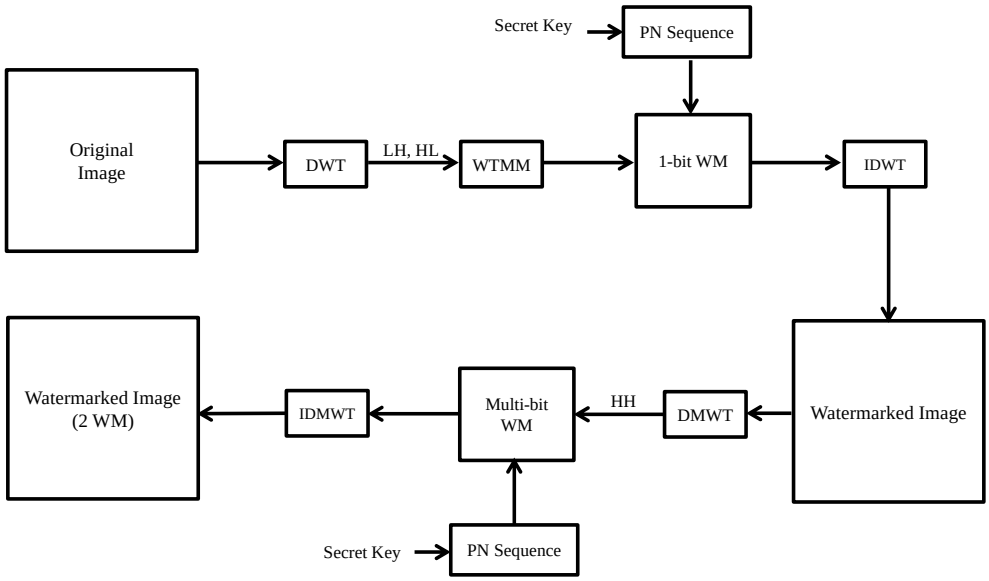


Figure 17 The overall proposed watermark embedding process.

As it is shown in Figure 17, DWT is first applied to the original image and the LH and HL sub-bands are used to calculate the WTMM and embed a 1-bit watermark.

The principle behind the WTMM and 1-bit watermark is that WTMM provides the (shift invariant) modulus maxima values, so that the 1-bit watermark can be embedded in the relevant shift invariant coefficients. The PN sequence corresponding to the 1-bit WM is generated based on a secret key. The purpose of embedding this 1-bit watermark is to improve the robustness of the proposed scheme against geometric attacks. Once the 1-bit watermark is embedded, the next step is to apply Inverse DWT to obtain the 1-bit watermarked image. Then, the DMWT is applied to the 1-bit watermarked image to access the High-High (HH) sub-band. The actual logo image which is the multi-bit watermark is then embedded in the HH sub-band with the help of a PN sequence and a secret key. Lastly, IDMWT is again applied to obtain the final watermarked image.

The embedding process is presented in more detail below. As shown in Figure 17, the overall embedding process includes computing the DWT of the original image first.

This is done as in [75]. Then, the LH and HL sub bands are extracted from the DWT of the original image. The magnitude $(Mf(s,x,y))$ and the angle $(Af(s,x,y))$ of the

WTMM are then calculated from the extracted LH and HL sub bands using Eq. (14) and Eq. (15) respectively.

A 1-bit watermark is then embedded in the WTMM coefficients using a PN sequence generated based on a secret key. The purpose of the 1-bit watermark is to improve robustness to geometrical attacks. The chip rate and (by implication) the robustness of the watermark is maximised by embedding just one single bit of data.

The logo (i.e. the multi-bit watermark) is then embedded in the HH sub-bands of the MW transform, again based on a PN sequence generated by a second secret key. As a result, the overall watermarked image contains two orthogonal watermarks (both the 1-bit and the multi-bit watermarks) embedded in different sub-bands using different transforms, which are being used for different purposes.

The motivation behind using two different watermarks is that the 1-bit watermark can be used to determine if the watermarked image has been attacked using a geometric attack, establish what the attack parameters were and undo this attack prior to the extraction of the logo. While spread-spectrum techniques possess many appealing properties [2], their main disadvantage is their sensitivity to any geometric attack that leads to 'desynchronization' between the resulting image and the generated PN sequence. Therefore, the proposed watermark embedding technique relies on the shift invariance property of the WTMM to embed a robust 1-bit watermark. The embedding of a 1-bit watermark is solely done as an attack detection mechanism, allowing the proposed watermarking scheme to undo the geometric transformation and 'resynchronize' the image prior to the recovery of the multibit WM. If the 1-bit watermark cannot be instantly recovered, this signals the presence of a geometric attack. In such a case, the geometric attack is first identified and then undone. Then, the proposed algorithm recovers the multi-bit logo (watermark).

The 1-bit watermark and multi-bit watermark embedding processes are illustrated in more detail in Figure 18 and Figure 19 respectively. Figure 18 shows the embedding process of the low capacity 1-bit watermark.

After embedding the high capacity watermark, the watermarked image is then split into its three colour components R, G, and B. DWT is applied on each colour component. This is followed by a step in which the LH, and HL sub-bands are extracted from each colour component. At the end of this step, six matrices corresponding to the LH and HL coefficients of each of the three colour components are obtained. Next, WTMM is computed for these components. The WTMM provides the (shift invariant) modulus maxima values, so that the 1-bit watermark can be embedded in the relevant shift invariant coefficients. For simplicity, these outputs can be merged together and treated as one large contiguous block (with a higher chip rate) for watermark insertion (and later detection) purposes. The 1-bit watermark is then embedded with respect to the PN sequence and a secret key. Lastly IDWT is applied to each of the colour component to obtain the final watermarked image.

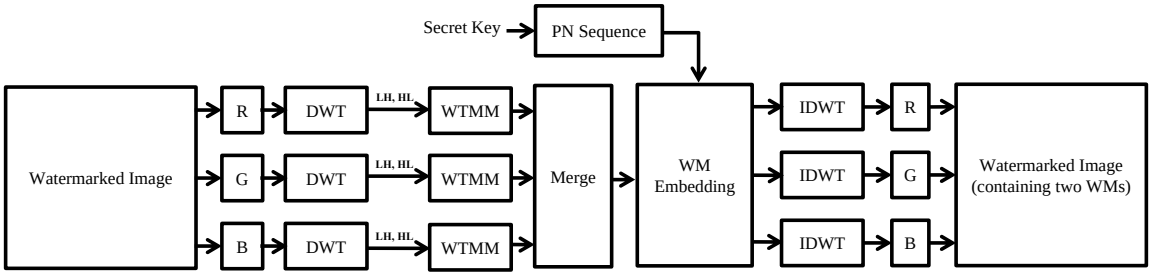


Figure 18 The proposed 1-bit watermark embedding process.

From Figure 19, it can be seen that for the embedding of the multi-bit watermark, the original image is first read. It is then split into its three colour components: Red, Green, and Blue represented by the ‘R’, ‘G’, and ‘B’ blocks respectively. Next, the HH sub-band is extracted from each of these components. This is followed by a step in which the HH sub-band coefficients of the R, G, and B components are merged into a large contiguous block. This effectively triples the chip rate reported to the size of the image.

The logo is then spread over the merged coefficients. This is done with the help of a PN sequence and a secret key. Lastly, IDWT is applied to get the watermarked image.

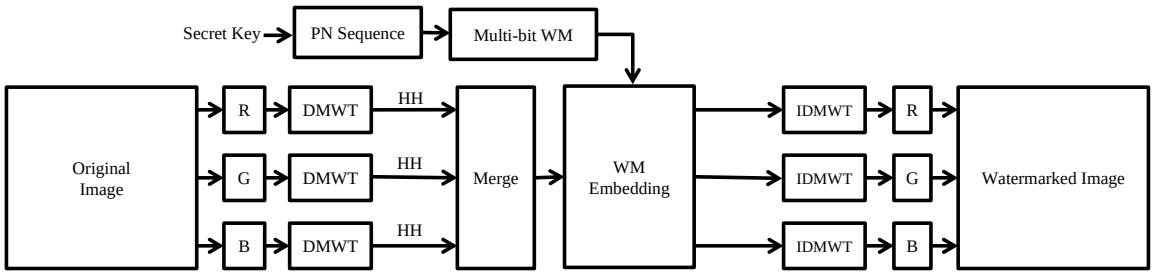


Figure 19 The proposed multi-bit watermark embedding process.

As it can be observed in Figure 18 and Figure 19, the DWT/DMWT is applied separately to each of the red, green, and blue components of an image. It is worth noting that by embedding the watermark into the RGB domain, the effective chip rate of the system is trebled.

5.2 Watermark Detection

The overall watermark recovery process is shown in Figure 20.

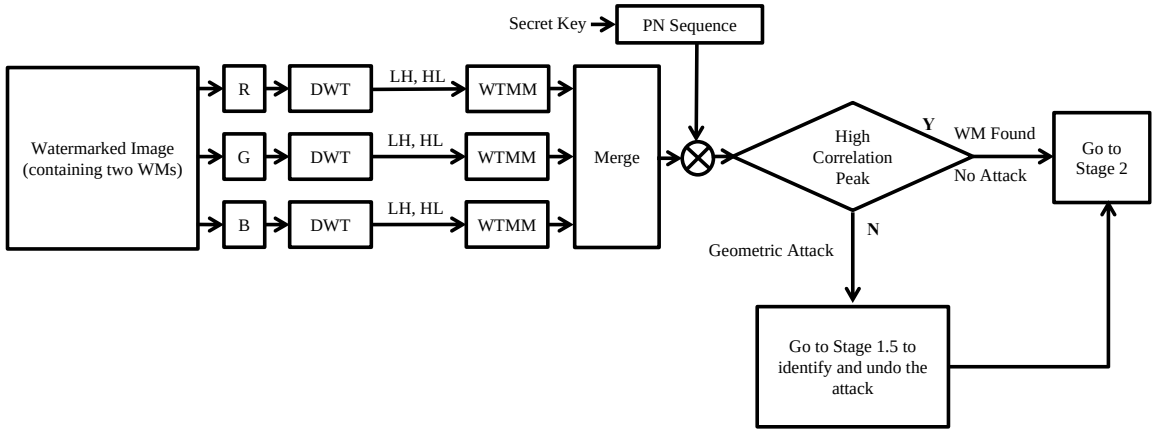


Figure 20 The proposed watermark recovery process.

Two scenarios have been considered for recovering the watermark. First, the 1-bit watermark is recovered. The recovered 1-bit watermark shows weather any attack on the watermarked image has taken place or not.

The process starts by reading the watermarked image and splitting it into its three colour components R, G, and B. The LH, HL sub-bands are then extracted and the WTMM is computed. This is followed by merging all coefficients in a large contiguous block just like for embedding. The 1-bit watermark is then recovered by cross-correlating the merged coefficients with the same PN sequence that was used for generating the 1-bit watermark. At this stage, if a single large cross-correlation peak is found, this signals that the watermarked image has not suffered any desynchronization attacks as a result of some geometrical attack and therefore the multi-bit watermark can be safely recovered.

In the second scenario, the single large peak is not found. Rather, many smaller peaks are observed. This indicates that there is something wrong with the watermarked image which has likely been subjected to a geometric attack. In this scenario, the attack needs to be identified and the watermarked image must be first corrected and brought back in sync with the PN sequence by undoing the geometrical transformation before being able to successfully recover the multi-bit watermark.

The multi-bit watermark recovery process is presented in Figure 21. First, the watermarked image is read. Then, it is split into its R, G, and B components. DWT is applied to each component. Then, the HH sib-band is extracted from each of the components. The coefficients are then merged. Finally, cross-correlation is computed between the merged coefficients and the same PN sequence that was generated during the embedding of the multi-bit watermark. Finally, the multi-bit watermark is recovered.

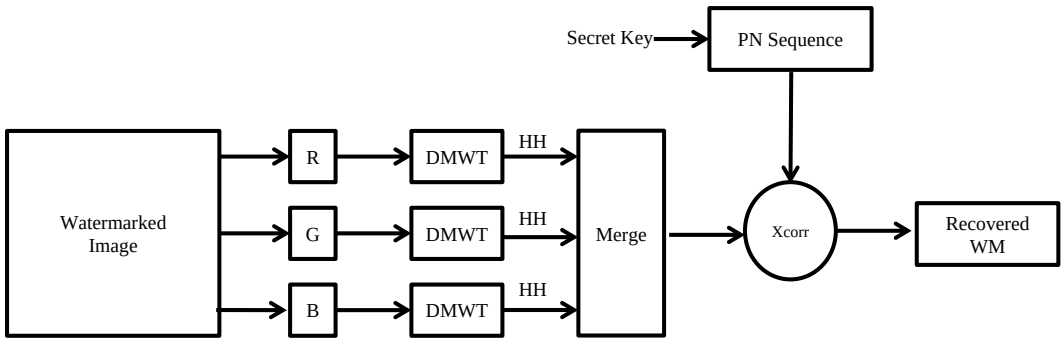


Figure 21 Stage 2 of the proposed watermark recovery scheme.

It should be noted that in Stage 2, the multi-bit watermark is blindly recovered via cross-correlation from the HH sub-bands of the red, green, and blue components of the watermarked image. The only data required for watermarking recovery is the watermarked image itself and the secret key used to generate the original PN sequence during embedding. This is one of the key advantages of spread spectrum based watermarking techniques.

As noted earlier, if during Stage 1 a single large cross-correlation peak cannot be found, then this outcome points to the scenario in which a geometric attack has taken place and the watermark recovery process enters an intermediate stage (Stage 1.5) designed to detect, undo the attack and resynchronize the watermark, before Stage 2 can be applied.

In the case of this second scenario, in which the watermarked image has been geometrically attacked, the steps taken to counter the manipulation and to recover the multi-bit watermark logo from the resynchronized watermarked image are shown in Figure 22. Attack parameters are determined via an extensive search carried out in a given attack parameter range. The attacked watermarked image is subjected to a number of successive geometrical transformations in this range. As shown in Figure 22, DWT is applied on both images and WTMM is computed. Cross-correlation is performed between the two outputs for each transform parameter in this range.

The transform parameters for which the cross-correlation peak is maximum represent the detected attack parameters.

This mechanism can be used to recover common geometrical transforms such as rotation, scaling and translation. Finally, once identified, the transform parameters are used to correct the attacked watermarked image, by undoing the attack and resynchronizing the watermark to allow the successful recovery of the logo at Stage 2.

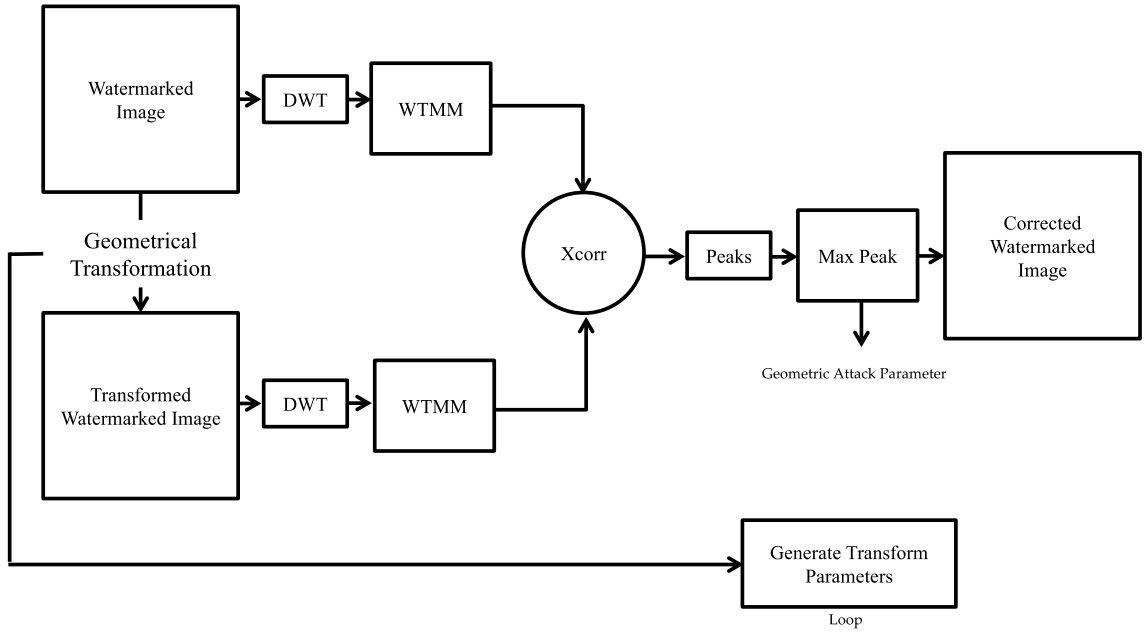


Figure 22 Stage 1.5 of the proposed watermark recovery process.

The search algorithm works as it follows. Once DWT and WTMM are computed, then cross-correlation of the WTMM of the attacked watermarked image and the WTMM of the rotated version of this image is repeatedly computed step by step and the value of each cross-correlation peak is recorded for each rotation step, as part of a loop. Once the loop completes, the rotation value that corresponds to the maximum recorded cross-correlation peak value amongst all other recorded cross-correlation values, represents the attack parameter itself.

Once the attack parameter has been identified in this way, this value is used to undo the attack and correct the geometrically attacked watermarked image.

Experimental results for various RST attacks and typical cross-correlation outputs for various images can be found in Chapter 6.

CHAPTER 6: RESULTS AND DISCUSSION

This chapter describes in detail the experimental setup, the experiments performed, and the results obtained. The experimental setup is described at the beginning of the chapter. The dataset used during the experiments is discussed next. This is followed by a discussion regarding the types of attacks used during simulations. Finally, the last section of this chapter focuses on presenting and discussing the detailed experimental results obtained for the proposed system.

6.1 Test Platform

In this section, the experimental setup of the research is presented. All the experiments were performed using MATLAB R2016. The experiments were performed on a MacBook Pro with a 2.2 GHz Intel Core i7 microprocessor, 16 GB DDR3 RAM, Intel Iris Pro 1536 MB graphics card and OS X El Capitan operating system.

6.2 Performance Evaluation Criteria

Three metrics were used to objectively evaluate the performance of the proposed algorithm. These are the Normalized Cross-Correlation (NCC), the Peak Signal-to-Noise Ratio (PSNR) and the Bit Error Rate (BER).

The reliability of watermark recovery can be objectively measured by explicitly computing the NCC between the recovered watermark and the originally embedded logo [82]. The NCC for an image I and a template I', can be calculated using Eq. (16) [76]

$$\gamma(u,v) = \frac{\sum_{x,y}\left[I(x,y)-\bar{I}_{u,v}\right]\left[I'(x-u,y-v)-\bar{I'}\right]}{\left\{\sum_{x,y}\left[I(x,y)-\bar{I}_{u,v}\right]^2 \sum_{x,y}\left[I'(x-u,y-v)-\bar{I'}\right]^2\right\}^{0.5}} \quad (16)$$

In Eq. (16), x and y represent the coordinates of the image, I while u and v represent the coordinates of the template I'. $\bar{I'}$ is the mean value of the template and $\bar{I}_{u,v}$ is the mean of $I(x,y)$ in the region under the template.

In the context of this work, NCC is applied between the original logo and the recovered logo to find the measure of similarity between these two images.

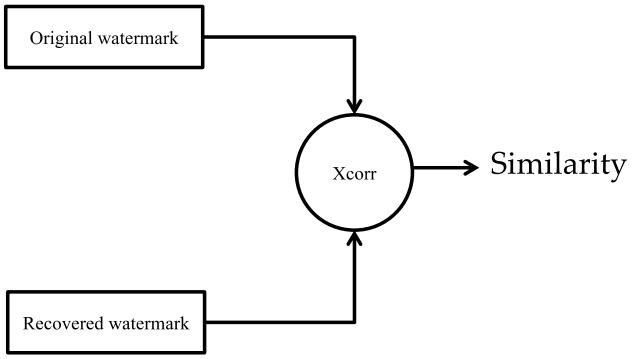


Figure 23 Normalized Cross-Correlation operation applied on the original watermark and the recovered watermark.

The PSNR has been traditionally used as a metric of choice to objectively evaluate image quality. In this thesis, it is used to evaluate the quality of the watermarked images. It can be mathematically calculated using Eq. (17).

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \tag{17}$$

In Eq. (17), MSE can be defined as:

$$MSE = \frac{1}{ab} \sum_{i=0}^{a-1} \sum_{j=0}^{b-1} [I(i,j) - J(i,j)]^2, \tag{18}$$

where I and J represent an original and a distorted image respectively while a and b represent the respective widths and heights of the images I and J.

Lastly, Bit Error Rate (BER) is another metric for determining the detection performance of a watermarking scheme. The BER is defined as the ratio between the number of incorrectly received bits divided by the total number of transferred bits during a certain transmission:

$$BER = \frac{number\ of\ incorrectly\ received\ bits}{total\ number\ of\ transferred\ bits} \tag{19}$$

6.3 Human Visual System Considerations

The Human Visual System (HVS) has been taken into consideration while assigning the embedding weights for the red, green, and blue components of the image. Many different weight combinations were empirically tested and it was concluded from the results that, the blue colour can be weighted higher than the red and green components. After experimenting with different weight factor combinations, the following weights were found to provide a good trade-off between robustness and quality of watermarked images: red (0.55), green (0.42), and blue (0.87). This weight assignment is also consistent with the fact that the human eye is more sensitive to changes in the green colour and least sensitive to changes in the blue colour.

Hence, the smallest weight has been assigned to the green colour (i.e. lowest embedding strength) while the largest weight has been assigned to the blue colour (i.e. highest embedding strength.).

6.4 Test Dataset

6.4.1 Cover Images

The test dataset for the experiments included 15 cover images most of which are well-known and publicly available. The resolutions of these images range from 256x256 to 512x512. These particular resolutions were selected based on the fact that these sizes are commonly used in the literature. Hence, for a fair comparison with state-of-the-art techniques, a dataset having similar resolutions was chosen. For each resolution, different images were used covering a broad range of characteristics. The details of the cover image test dataset are presented in Table 1, Figure 24 and Figure 25.

Table 1 Cover image test dataset

Image	Resolution
Lena	512x512
Pepper	512x512
Barbara	512x512
Airplane	512x512
Sailboat	512x512
Parrot2	512x512
Parrot	512x512
Colors	512x512
Flower	512x512
Natural	512x512
Pepper3	512x512
Fruits	512x512
Lena	256x256
Pepper2	256x256
Foods	256x256

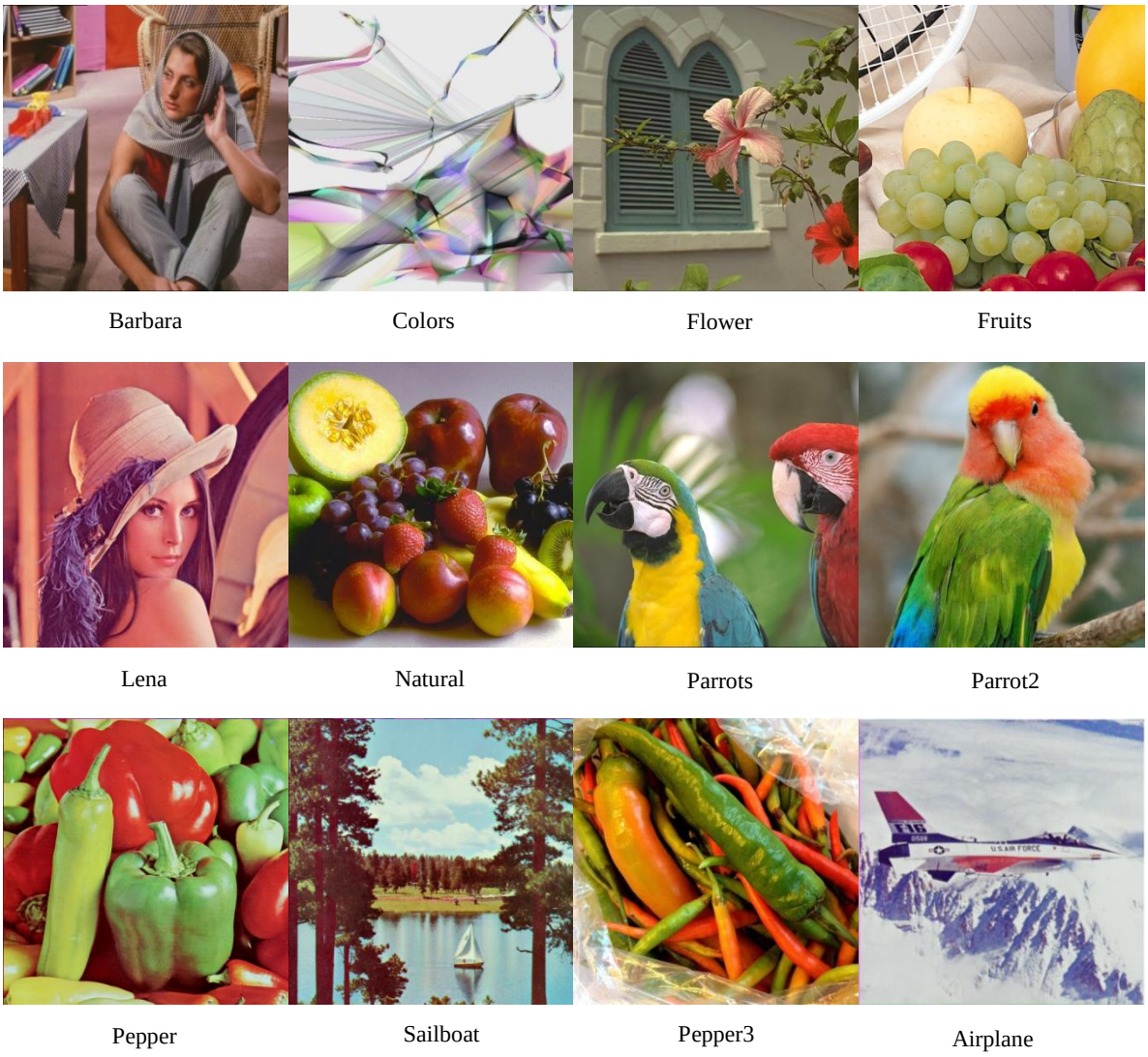


Figure 24 Cover images of resolution 512x512.

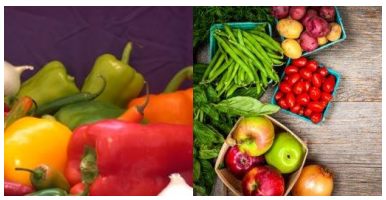


Figure 25 Cover images of resolution 256x256.

6.4.2 Logo Images

Two different black and white (1 bit per pixel) logo images of different sizes were used. These are the 'TEST' logo image which has 50×20 pixels and the 'ME' logo image which has 21×10 pixels. These logos translate to a watermark length of 1000 bits and respectively 210 bits. Black and white logo images were chosen to keep the watermark length manageable. The logo images are shown in Figure 26 and Figure 27.

Figure 26 The 'TEST' logo image

Figure 27 The 'ME' logo image

6.4.3 Chip Rate

Chip rate (CR) can be mathematically defined as:

$$CR = \frac{w \times h}{N}$$

Where w and h are the width and height of the host image while N is the length of the number of bits of the watermark (in this case, the binary logo or the 1-bit watermark).

Since, two orthogonal watermarks are used in the proposed scheme, there would be two separate chip rates for each watermark.

Single-bit watermark

In case of the single-bit watermark, in order to calculate the chip rate, it is important to identify the number of significant WTMM coefficients of the LH and HL sub-bands of each of the Red, Green, and Blue components, since the watermark is only embedded in these coefficients. For the 512x512 Lena image, there relevant WTMM coefficients are:

$$LH(Red) = 1393\ coefficients$$

$$HL(Red) = 1393\ coefficients$$

$$Total\ (Red) = 2786\ coefficients$$

$$LH(Green) = 1351\ coefficients$$
$$HL(Green) = 1351\ coefficients$$
$$Total\ (Green) = 2702\ coefficients$$

$$LH(Blue) = 1351\ coefficients$$
$$HL(Blue) = 1351\ coefficients$$
$$Total\ (Blue) = 2702\ coefficients$$

$$Chip\ Rate\ (Single\ bit\ WM) = Total\ (Red) + Total\ (Green) + Total\ (Blue)$$
$$\boldsymbol{Chip\ Rate\ (Single\ bit\ WM) = 8,190}$$

Multi-bit watermark

In case of the multi-bit watermark, the watermark is embedded in the HH sub-bands. Hence, to find the chip rate, first, the number of coefficients in the HH sub-bands of each colour component are found i.e.,

$$HH(Red) = 4096\ coefficients$$
$$HH(Green) = 4096\ coefficients$$
$$HH(Blue) = 4096\ coefficients$$
$$Total\ number\ of\ coefficients = HH\ (Red) + HH\ (Green) + HH\ (Blue)$$
$$= 12{,}288\ coefficients$$
$$Chip\ Rate = \frac{w \times h}{N}$$

In case of the 'TEST' logo, the size of the logo is 50×20. Hence, $length = 1{,}000$.

$$Chip\ Rate = \frac{12{,}288}{1{,}000}$$
$$\boldsymbol{Chip\ Rate\ (Multi\ bit\ WM) = 12.288}$$

6.5 Attack Types

The main focus of the experiments is on demonstrating the robustness of the proposed algorithm against geometric attacks. These attacks include rotation, scaling and translation. For testing robustness against rotation, the images are rotated by different angles from 1 degree to 359 degrees and for each rotated angle the watermark is detected and recovered. Similarly, for testing robustness against translation, the image is shifted using different pixel offset values and in each case the watermark is detected and recovered. Lastly, to test the robustness of the proposed algorithm against scaling, the image is scaled both up and down by different scaling factors and in each case the watermark is detected and recovered.

6.6 Results and Discussion

This section provides the overall results for the proposed technique for a variety of circumstances and for a variety of attacks. Section 6.6.1 discusses the results for watermark recovery in case of no attack. Section 6.6.2 discusses the results of watermark detection and recovery in case of rotation, scaling and translation attacks. Comparative results using other wavelets are presented in Section 6.6.3. The performance of the proposed watermarking scheme is compared against other state-of-the-art watermarking schemes in the Section 6.6.4. Finally, an overall summary of the results is presented in Section 6.6.5.

6.6.1 Watermark Recovery in Case of No Attack

This section presents the results of the proposed method in the simplest case when no attack has taken place. The results of this case are demonstrated by embedding a watermark in an image and then recovering it. The fidelity of the recovered watermark is measured using Normalized Cross-Correlation (NCC). Watermarked image quality is assessed by calculating the PSNR between the original and the watermarked image.

Figure 28 shows the detection result for the 1-bit watermark. It can be seen from Figure 28 that since a peak value of 1 has been achieved, with no side peaks, no geometrical attack has been detected, and the 1-bit watermark is successfully extracted, indicating

that no attack took place and that it is safe to proceed to Stage 2 and recover the embedded logo.

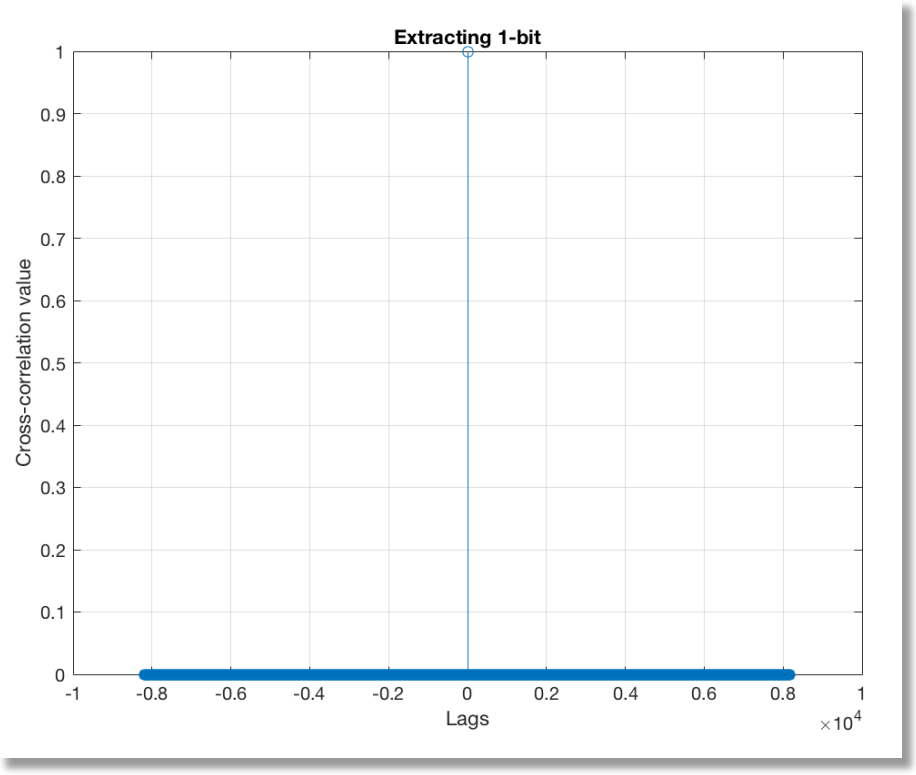


Figure 28 The detection of 1-bit watermark.

It is worth noting that the profile of NCC values can also indicate that a desynchronization type attack took place and therefore the logo watermark image cannot be recovered without first resynchronizing the image by undoing the attack.

A typical example of this is illustrated in Figure 29 where many peaks of similar amplitudes can be seen. The presence of many peak values indicates that the watermarked image has been subjected to manipulation and that it needs to be corrected before the actual logo watermark image can be recovered.

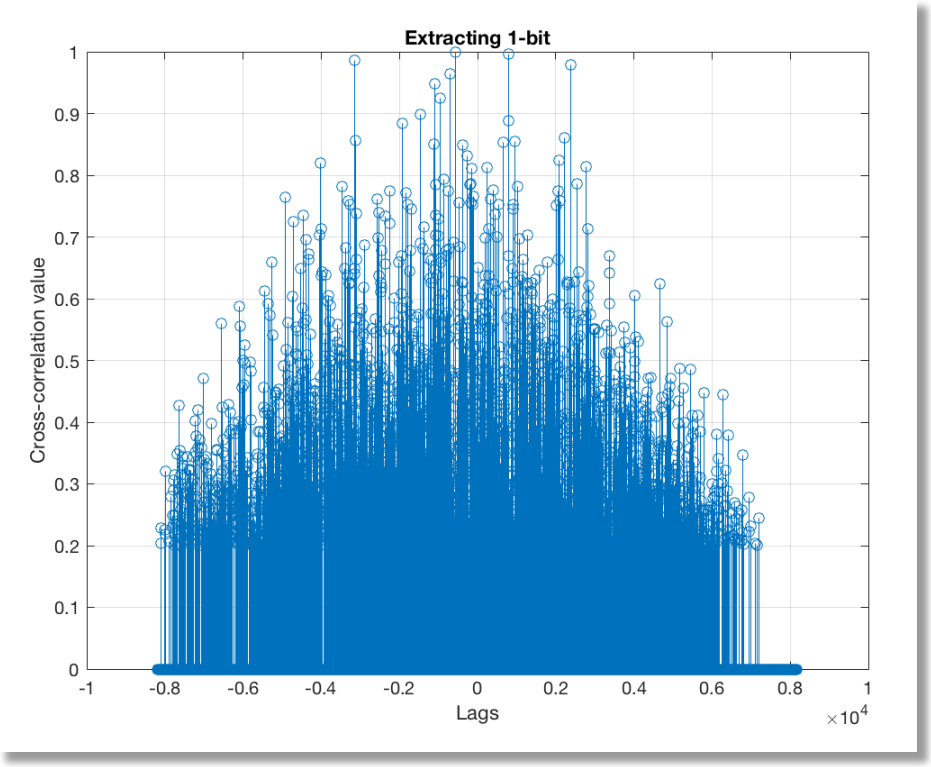


Figure 29 In case of an attack, the NCC profile shows many peaks.

The results for the recovery of the multi-bit watermark are shown in Table 2 for the 'TEST' logo image and in Table 3 for the 'ME' logo image and the wavelet type is Multiwavelet Cardbal2.

Table 2 Recovering the logo watermark in case of no attack. The results are shown for the 512x512 resolution images, the 'TEST' logo and the Cardbal2 balanced multiwavelet.

Image	PSNR (dB)	Normalized Cross-Correlation (NCC)	Bit Error Rate (BER)
Fruits	36.14	0.99	0.001
Pepper3	37.89	1	0
Flower	36.29	1	0
Parrot	36.63	1	0
Natural	36.87	1	0
Parrot2	37.46	1	0
Colors	36.43	1	0
Sailboat	35.64	1	0
Lena	37.24	1	0
Pepper	37.29	1	0
Barbara	36.44	1	0
Airplane	36.67	1	0

Table 3 Recovering the logo watermark in case of no attack. The results are shown for the 512x512 resolution images, the 'ME' logo and the Cardbal2 balanced multiwavelet.

Image	PSNR (dB)	Normalized Cross-Correlation (NCC)	Bit Error Rate (BER)
Lena	42.447	1	0
Barbara	40.423	1	0
Pepper	42.216	1	0
Airplane	40.978	1	0
Parrot2	42.963	1	0
Natural	40.915	1	0
Fruits	39.531	1	0
Parrot	40.459	1	0
Sailboat	38.666	1	0

Next, a comparison of results obtained using different types of wavelet and multiwavelet filter banks is showed. The results are shown for two different watermark sizes.

Figure 30 shows several 'Lena' watermarked images (of size 512x512) watermarked with the 'TEST' logo which has been embedded using different type of wavelet and multiwavelet filters: Cardbal2, GHM, BAT02, Daubechies (d4), and Antonini 7.9. The PSNR values obtained for each image are: Cardbal2 (37.244 dB), GHM (37.073 dB), BAT02 (37.077 dB), Daubechies (d4) (34.464 dB), and Antonini 7.9 (34.319 dB).

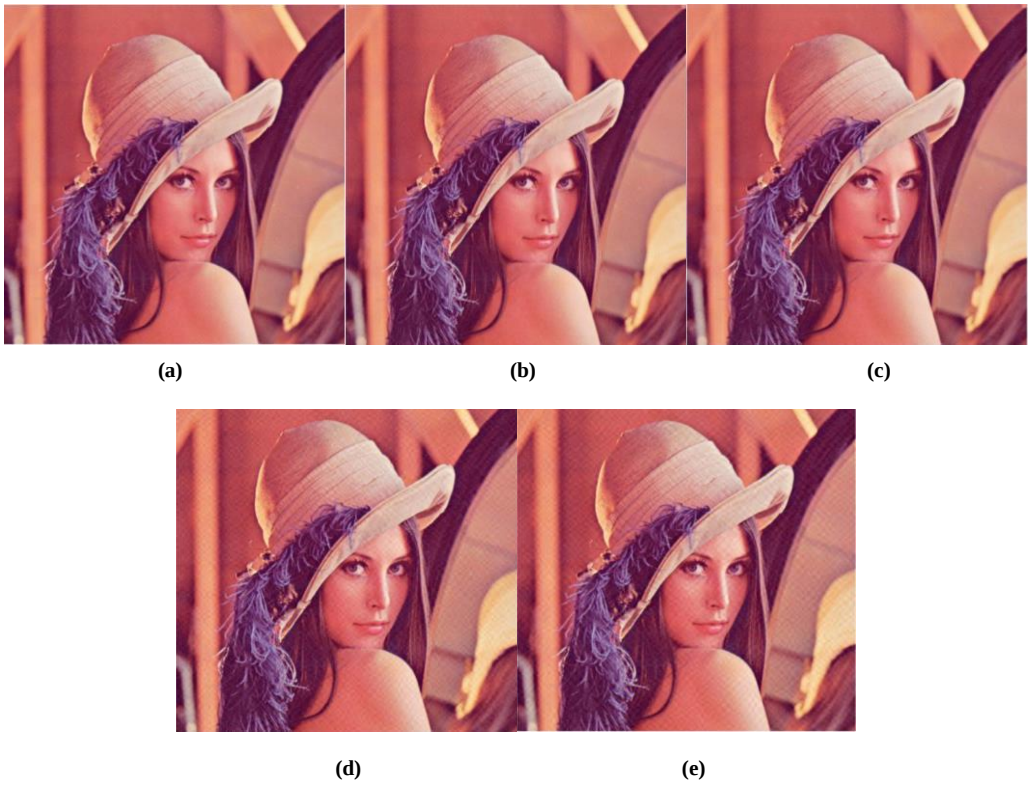


Figure 30 Watermarked Lena images using the following wavelets: (a) Cardbal2; (b) GHM; (c) BAT02; (d) Daubechies (d4); and (e) Antonini 7.9.

In terms of robustness, it can be observed that the Cardbal2, GHM and BAT02 multiwavelets filters achieve an NCC value of 1, followed by the Daubechies (d4) and Antonini 7.9 wavelet filters with an NCC value of 0.98 (See Figure 31).

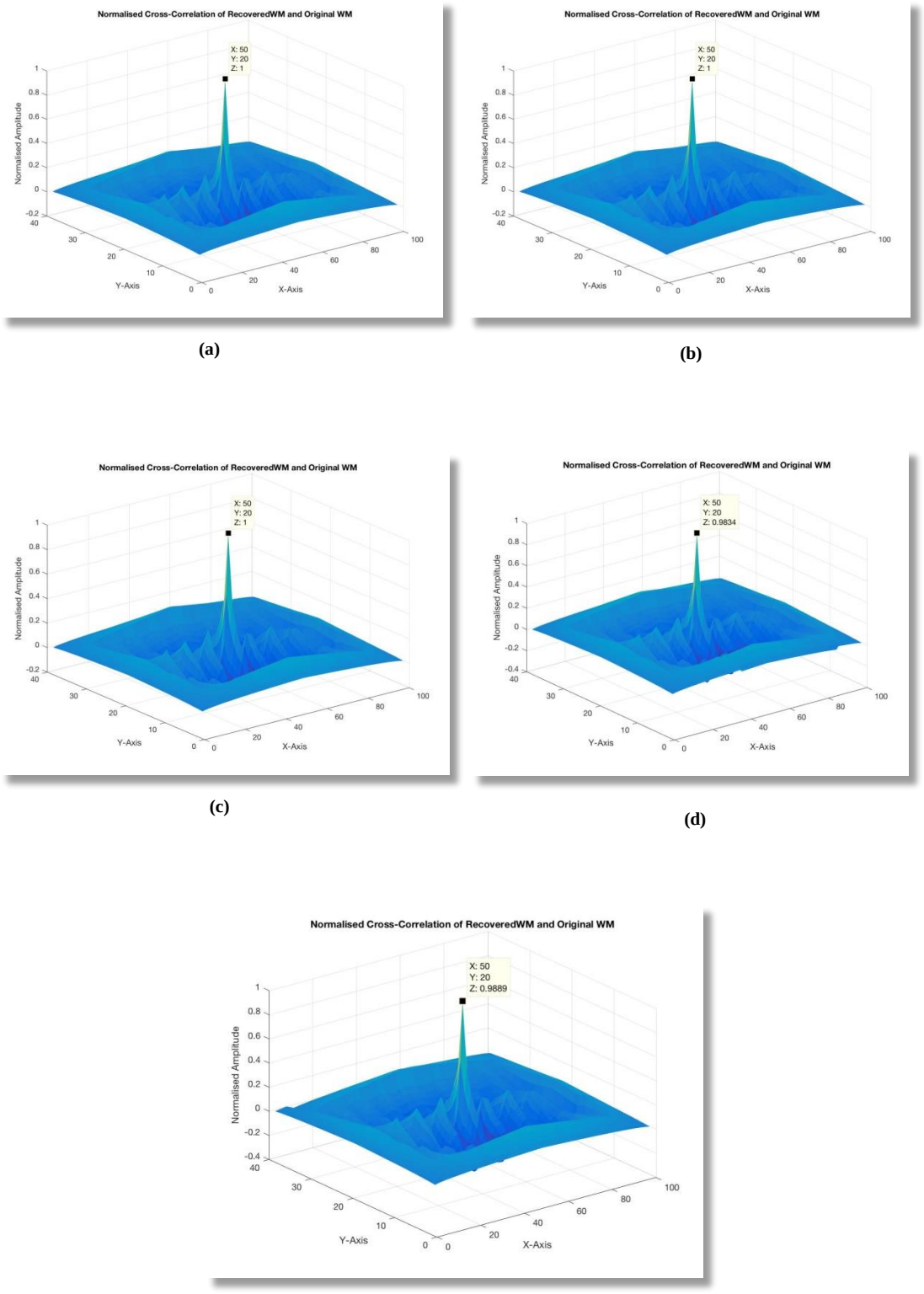


Figure 31 Normalized Cross-correlation (NCC) results between the recovered and the original logos after a rotation attack for image Lena using: (a) Cardbal2; (b) GHM; (c) BAT02; (d) Daubechies (d4); and (e) Antonini 7.9.

It can be seen from Figure 31 and the results provided in Table 2 and Table 3, that the proposed watermarking scheme can, as expected, easily and efficiently recover watermarks in the normal case where no attack has taken place. Experiments were performed using other types of wavelets as well but the multiwavelets were found to produce the best results. Comparisons of the results obtained using the Cardbal2, GHM, and BAT02 multiwavelets, as well as the Antonini 7.9 and Daubechies (d4) scalar wavelets and are shown in Figure 32 and Figure 33.

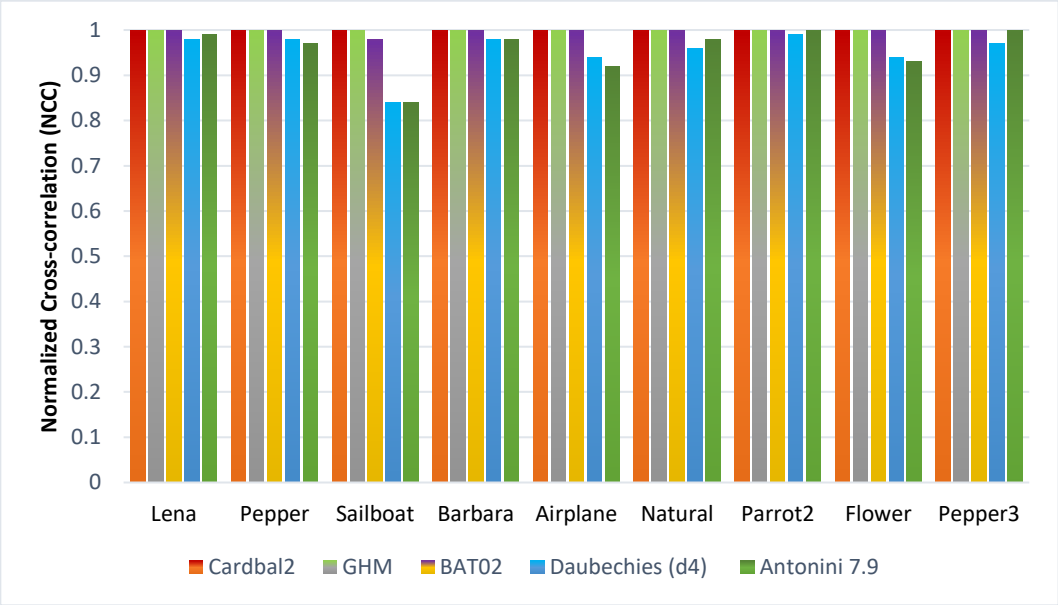


Figure 32 Comparison of the results obtained using different types of wavelets/multiwavelets. The results are shown for 512x512 resolution images and the 'TEST' logo watermark.

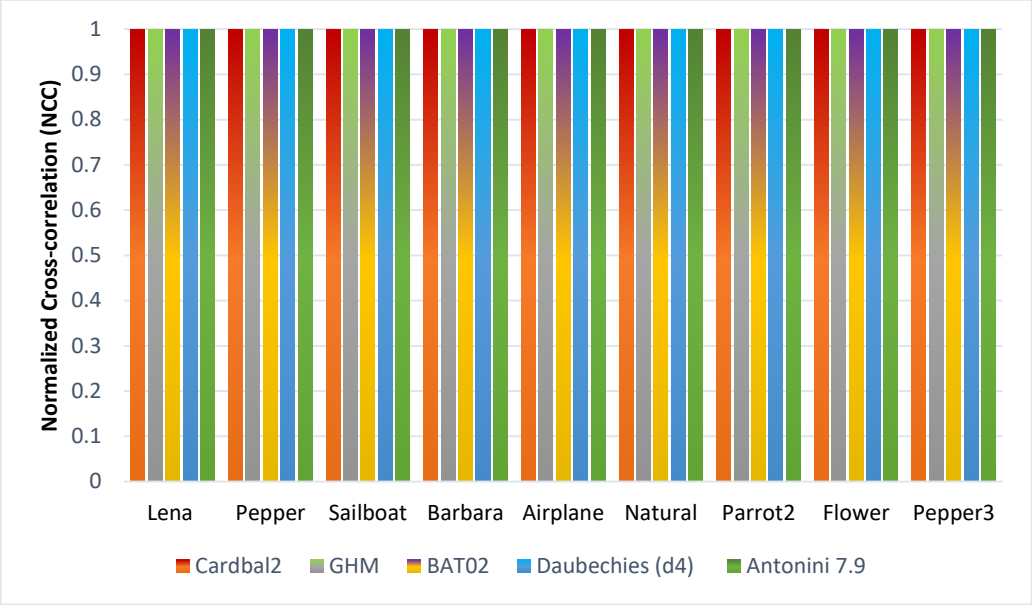


Figure 33 Comparison of the results obtained using different types of wavelets/multiwavelets. The results are shown for 512x512 resolution images and the smaller 'ME' logo watermark.

The results presented in Figure 32 and Figure 33, show that the Cardbal2 and GHM multiwavelets offer the best results. Moreover, it can be observed from Figure 32 and Figure 33 that multiwavelets achieve relatively stable NCC values compared to the other wavelet types. For example, for the 'TEST' logo in Figure 32, the NCC values for multiwavelets (Cardbal2, GHM, and BAT02) deviate between 0.98 and 1. On the other hand, for Daubechies (d4), the range is from 0.84 to 0.98 while for Antonini 7.9, the range is from 0.84 to 0.99. On the other hand, for the 'ME' logo, all the test wavelet types, including multiwavelets, Daubechies (d4), and Antonini 7.9 achieve NCC values of 1 (See Figure 33).

Figure 34 and Figure 35 present the Peak Signal-to-Noise Ratio (PSNR) comparison results for the three types of wavelets/multiwavelets for the 'TEST' and 'ME' logo images respectively. Figure 34 shows the Peak Signal-to-Noise Ratio (PSNR) comparison results for the 'TEST' logo watermark. The PSNR range for watermarked images using Cardbal2 multiwavelet is between 35.6 dB to 37.8 dB; for the GHM, between 35.3 dB to 37.8 dB; for the BAT02, between 35.4 dB to 37.6 dB; for the Daubechies (d4), between 30.5 dB to 34.9 dB; and for the Antonini 7.9, between 30.7 dB to 35.1 dB.

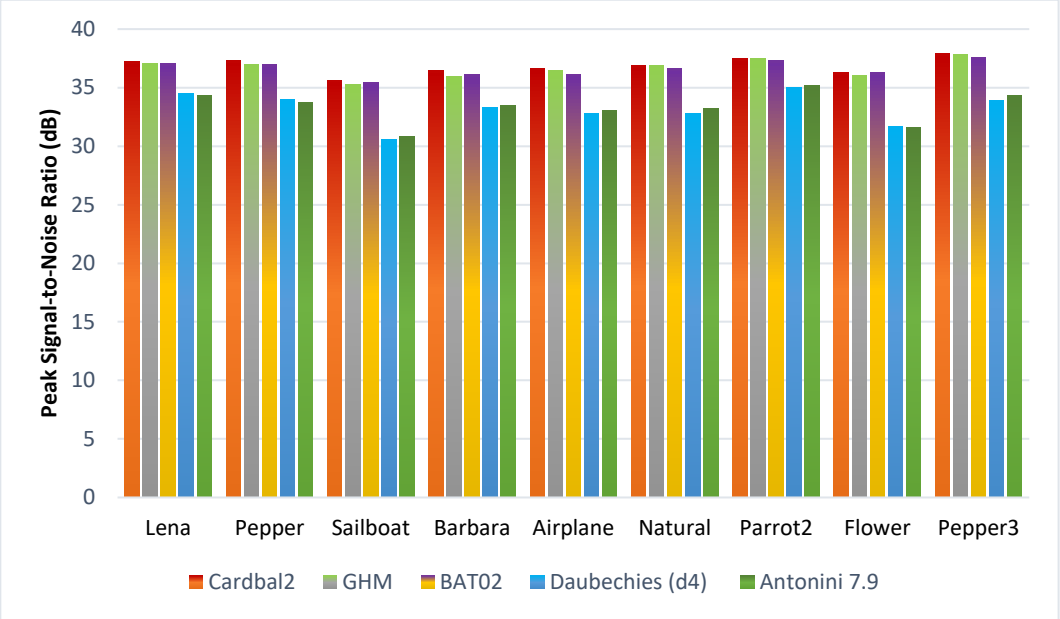


Figure 34 Comparison of PSNR results for different types of wavelets/multiwavelets. The results are shown for 512x512 resolution images and the 'TEST' logo watermark.

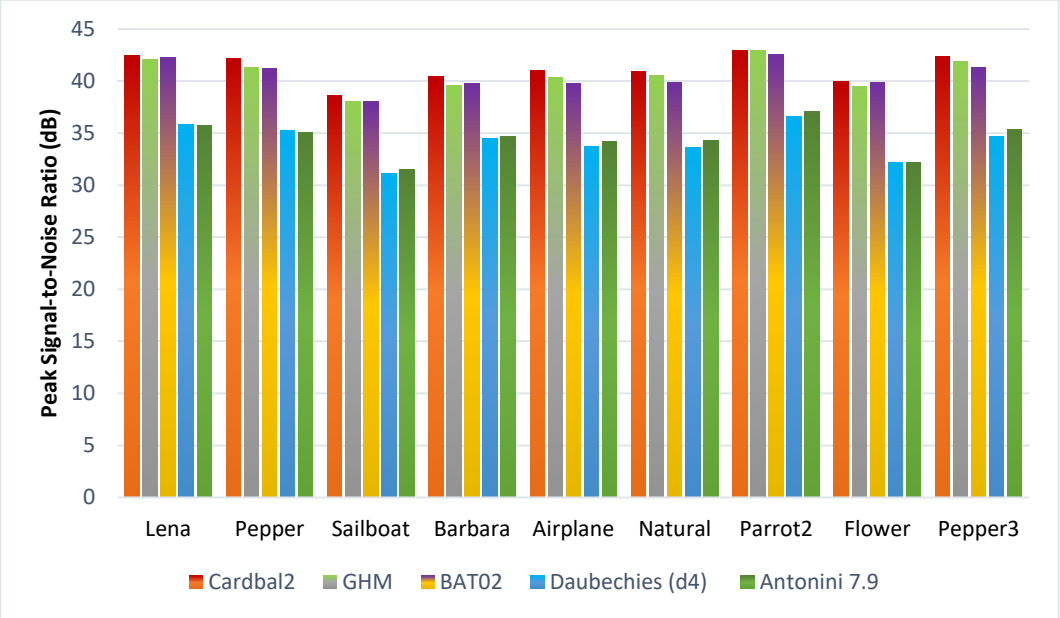


Figure 35 Comparison of PSNR results for different types of wavelets/multiwavelets. The results are shown for 512x512 resolution images and the smaller 'ME' logo watermark.

6.6.2 Watermark Detection and Recovery in Case of an Attack

The proposed watermarking scheme can efficiently detect watermarks even after the cover image has undergone geometric attacks of varying intensities. This section demonstrates the watermark detection and recovery capabilities of the proposed watermarking scheme for both image sizes of 512x512 and 256x256 using the Cardbal2 multiwavelet.

For this purpose, both the 1-bit and multi-bit (logo) watermarks are first embedded in a cover image. The watermarked image is then subjected to rotation, translation, and scaling and in each case the proposed scheme is used to find the right transform parameters and undo them. The results in Table 4 and Table 5 demonstrate the capability of the proposed method to detect the amount of rotation, scaling, or translation that the watermarked image is subjected to.

The results in Table 4 are for cover images of resolution 512x512 while those in Table 5 are for cover images of resolution 256x256. In both the cases, the 'TEST' logo watermark is used. Table 4 shows 12 different watermarked images under RST attacks.

With the help of WTMM and cross-correlation, the parameters of the geometric distortions are detected, as per Step 1.5 of the proposed scheme. The rotation attack section shows the watermarked image rotated by various degrees such as 0.5, 10.5, 160.2 degrees and how these distortion parameters are successfully detected. For the scaling attack, the watermarked image is scaled by different scaling factors such as 0.75 and 1.35 and the values of these scaling factors are then detected. Similarly, for translation, the watermarked image is subjected to various translation offset values which are then successfully detected.

Table 4 Distortion parameter detection using the proposed method. 'D' represents the 'Detected Parameter' and 'N' represents the 'Normalized Cross-Correlation Coefficient'. Results are shown for the 512x512 resolution images, the 'TEST' logo and the Cardbal2 balanced multiwavelet.

Attack / Image		Lena		Pepper		Barbara		Airplane		Sailboat		Parrot2	
Distortion Parameter		D	N	D	N	D	N	D	N	D	N	D	N
Rotation	0.5º	0.5º	1	0.5º	1	0.5º	1	0.5º	1	0.5º	1	0.5º	1
	10.5º	10.5º	1	10.5º	1	10.5º	1	10.5º	1	10.5º	0.98	10.5º	1
	40º	40º	0.98	40º	1	40º	0.99	40º	0.95	40º	0.97	40º	0.98
	90º	90º	1	90º	1	90º	1	90º	1	90º	1	90º	1
	120º	120º	0.98	120º	1	120º	1	120º	0.99	120º	0.98	120º	1
	160.2º	160.2º	1	160.2º	1	160.2º	1	160.2º	1	160.2º	0.99	160.2º	1
	250.8º	250.8º	1	250.8º	1	250.8º	1	250.8º	1	250.8º	0.99	250.8º	1
	300º	300º	1	300º	1	300º	1	300º	0.99	300º	0.98	300º	1
Scaling Factor	0.5	0.5	1	0.5	1	0.5	0.97	0.5	1	0.5	0.95	0.5	1
	0.75	0.75	1	0.75	1	0.75	0.98	0.75	1	0.75	0.98	0.75	1
	1.25	1.25	1	1.25	1	1.25	1	1.25	1	1.25	1	1.25	1
	1.35	1.35	0.99	1.35	0.99	1.35	0.97	1.35	0.99	1.35	0.97	1.35	1
	1.4	1.4	0.99	1.4	0.98	1.4	0.94	1.4	0.99	1.4	0.94	1.4	1
Translation (x, y)	(0, 10)	(0, 10)	1	(0, 10)	1	(0, 10)	1	(0, 10)	1	(0, 10)	0.99	(0, 10)	1
	(48, 48)	(48, 48)	1	(48, 48)	1	(48, 48)	1	(48, 48)	0.99	(48, 48)	1	(48, 48)	1
	(96, 96)	(96, 96)	1	(96, 96)	1	(96, 96)	1	(96, 96)	0.99	(96, 96)	0.97	(96, 96)	1
	(128, 128)	(128, 128)	0.99	(128, 128)	1	(128, 128)	0.98	(128, 128)	0.99	(128, 128)	0.98	(128, 128)	1
	(176, 176)	(176, 176)	1	(176, 176)	0.99	(176, 176)	0.94	(176, 176)	1	(176, 176)	0.94	(176, 176)	1

Attack / Image		Lena		Pepper		Barbara		Airplane		Sailboat		Parrot2	
Distortion Parameter		**D**	**N**	**D**	**N**	**D**	**N**	**D**	**N**	**D**	**N**	**D**	**N**
Rotation	0.5º	0.5º	1	0.5º	1	0.5º	1	0.5º	0.99	0.5º	1	0.5º	1
	10.5º	10.5º	1	10.5º	1	10.5º	0.98	10.5º	0.98	10.5º	1	10.5º	0.99
	40º	40º	0.98	40º	0.98	40º	0.95	40º	0.98	40º	0.97	40º	0.98
	90º	90º	1	90º	1	90º	1	90º	0.99	90º	1	90º	1
	120º	120º	1	120º	0.99	120º	0.98	120º	1	120º	1	120º	0.99
	160.2º	160.2º	1	160.2º	1	160.2º	0.99	160.2º	0.98	160.2º	1	160.2º	0.99
	250.8º	250.8º	1	250.8º	1	250.8º	0.99	250.8º	0.98	250.8º	1	250.8º	0.99
	300º	300º	1	300º	0.99	300º	0.98	300 º	1	300 º	1	300 º	0.99
Scaling Factor	0.5	0.5	1	0.5	1	0.5	0.99	0.5	0.98	0.5	0.99	0.5	1
	0.75	0.75	1	0.75	1	0.75	0.98	0.75	0.97	0.75	1	0.75	0.98
	1.25	1.25	1	1.25	1	1.25	0.99	1.25	0.99	1.25	1	1.25	0.98
	1.35	1.35	1	1.35	0.99	1.35	0.98	1.35	0.94	1.35	1	1.35	0.97
	1.4	1.4	1	1.4	0.98	1.4	0.98	1.4	0.94	1.4	1	1.4	0.97
Translation (x, y)	(0, 10)	(0, 10)	1	(0, 10)	1	(0, 10)	1	(0, 10)	0.98	(0, 10)	1	(0, 10)	1
	(48, 48)	(48, 48)	1	(48, 48)	1	(48, 48)	1	(48, 48)	0.97	(48, 48)	1	(48, 48)	0.98
	(96, 96)	(96, 96)	1	(96, 96)	1	(96, 96)	0.99	(96, 96)	0.98	(96, 96)	0.99	(96, 96)	0.98
	(128, 128)	(128, 128)	1	(128, 128)	0.99	(128, 128)	0.98	(128, 128)	0.98	(128, 128)	0.98	(128, 128)	0.98
	(176, 176)	(176, 176)	1	(176, 176)	0.95	(176, 176)	0.95	(176, 176)	0.97	(176, 176)	0.97	(176, 176)	0.98

The original distortion parameters and the detected distortion parameters for all 512x512 images are shown in Figure 36 – Figure 39. The results in Figure 36 – Figure 39 show that thanks to the 1-bit watermark, the proposed watermarking scheme can successfully detect the distortion parameters for rotation, scaling, and translation.

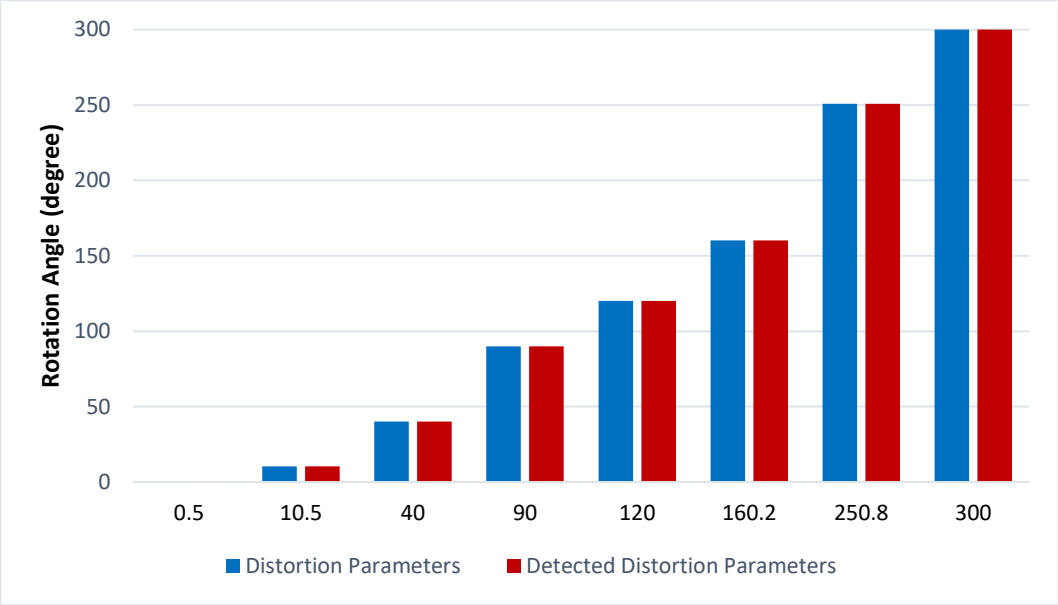


Figure 36 Original distortion parameters and the detected distortion parameters for rotation attacks.

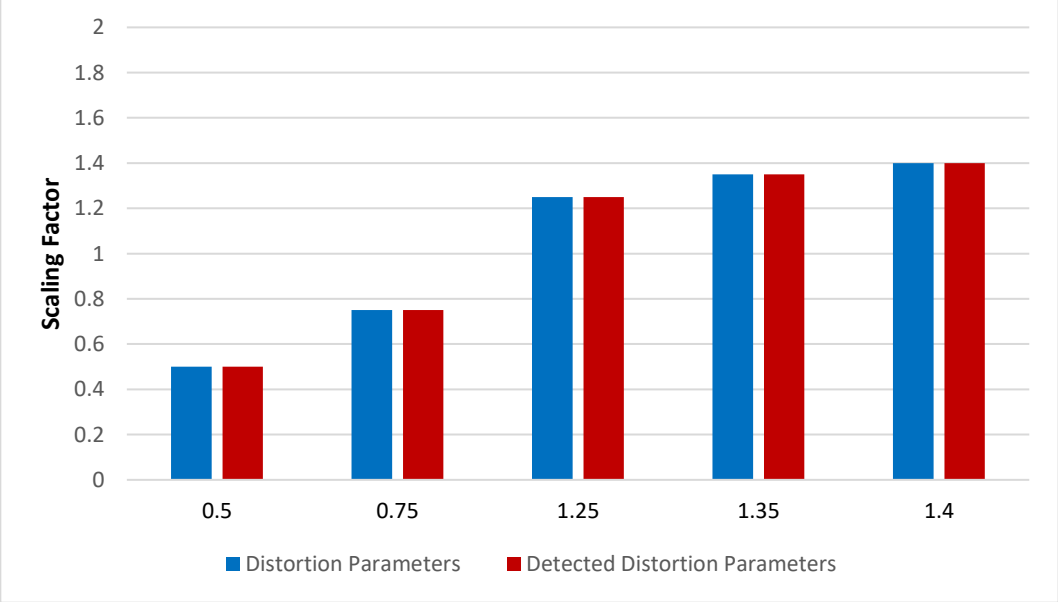


Figure 37 Original distortion parameters and the detected distortion parameters for scaling attacks.

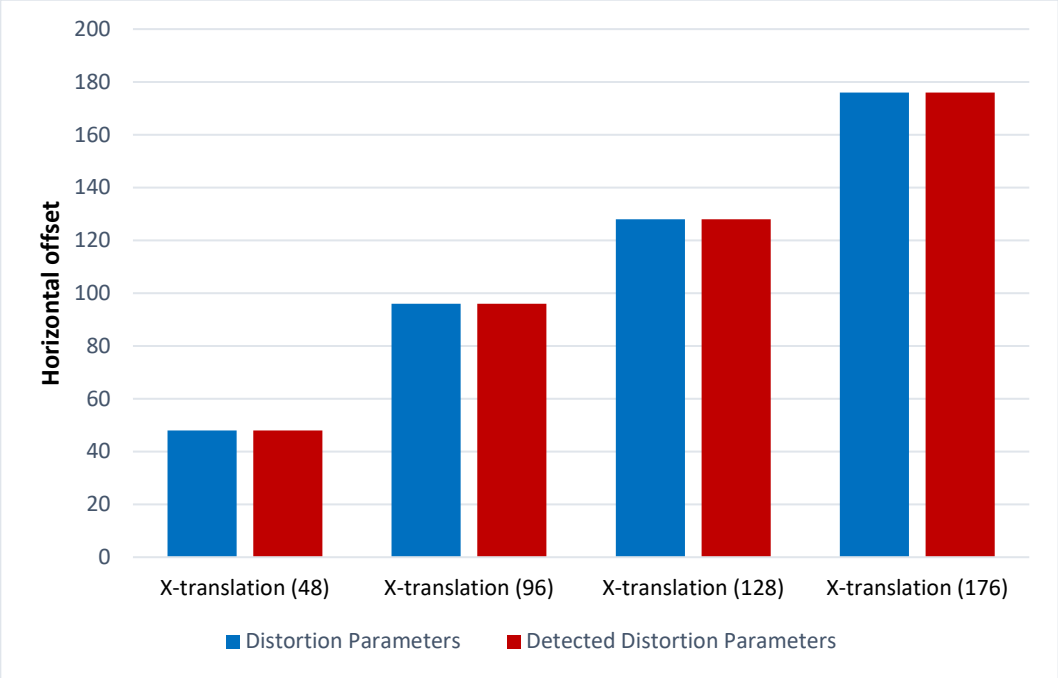


Figure 38 Original distortion parameters and the detected distortion parameters for translation attacks (horizontal shifts).

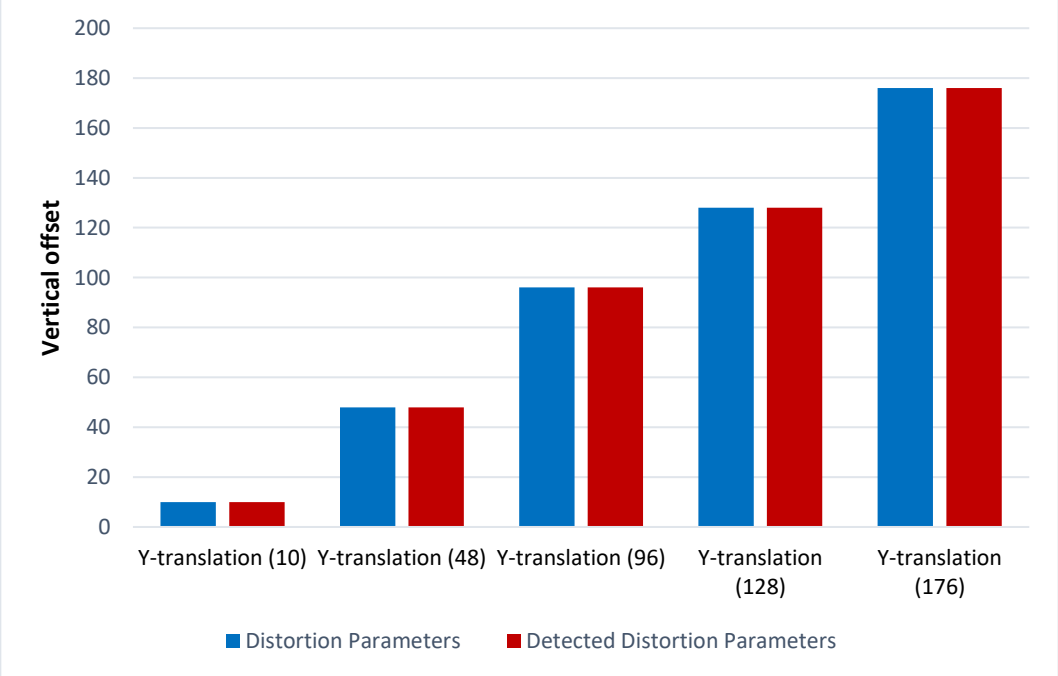


Figure 39 Original distortion parameters and the detected distortion parameters for translation attacks (vertical shifts).

Similar results are obtained for 256x256 resolution images. Table 5 shows the results for the case when smaller watermarked images of size 256x256 are subjected to geometrical attacks. This is to see the effect of using smaller cover size images. For all the RST attacks, the algorithm has managed to detect the distortion transform parameters successfully. These results are summarized in Table 5.

Table 5 Distortion parameter detection using the proposed method. 'D' represents the 'Detected Parameter' and 'N' represents the 'Normalized Cross-Correlation Coefficient'. Results are shown for the 256x256 resolution images, the 'TEST' logo image and the Cardbal2 balanced multiwavelet.

Attack / Image		Lena		Pepper2		Foods	
Distortion Parameter		**D**	**N**	**D**	**N**	**D**	**N**
Rotation (Degrees)	0.7°	0.7°	1	0.7°	1	0.7°	1
	7.5°	7.5°	1	7.5°	1	7.5°	1
	45°	45°	0.93	45°	0.98	45°	0.91
	90°	90°	1	90°	1	90°	1
	130°	130°	0.99	130°	0.98	130°	0.95
	180.6°	180.6°	1	180.6°	1	180.6°	1
	350°	350°	1	350°	1	350°	1
Scaling Factor	0.85	0.85	0.96	0.85	0.96	0.85	0.87
	1.1	1.1	1	1.1	1	1.1	1
	1.35	1.35	1	1.35	1	1.35	0.99
	1.4	1.4	1	1.4	1	1.4	0.99
	1.6	1.6	0.99	1.6	1	1.6	1
Translation (x, y)	(40, 40)	(40, 40)	1	(40, 40)	1	(40, 40)	1
	(80, 80)	(80, 80)	1	(80, 80)	1	(80, 80)	1
	(120, 120)	(120, 120)	1	(120, 120)	1	(120, 120)	0.99

6.6.2.1 Rotation Attacks

This section covers in more detail the experimental results for rotation attacks. The rotation attack was tested using two image sizes: 512x512 and 256x256. The logo has been embedded using the Cardbal2 multiwavelet. The watermarked images were attacked by applying different degrees of rotation for both image sizes. Figure 40 shows a number of examples for various images. Stage 1.5 of the proposed algorithm is applied in order to detect the amount of rotation and undo the geometric attack. The corresponding normalized cross-correlation results used to detect the parameters of the attack for each image are shown in Figure 41. The position of the maximum value of the cross-correlation peaks indicates the amount of rotation detected for each image. Figure 42 shows the restored images after undoing the rotation attacks by using the attack parameters detected as a result of applying the Stage 1.5 algorithm as illustrated in Figure 41, for each attacked image shown in Figure 40.

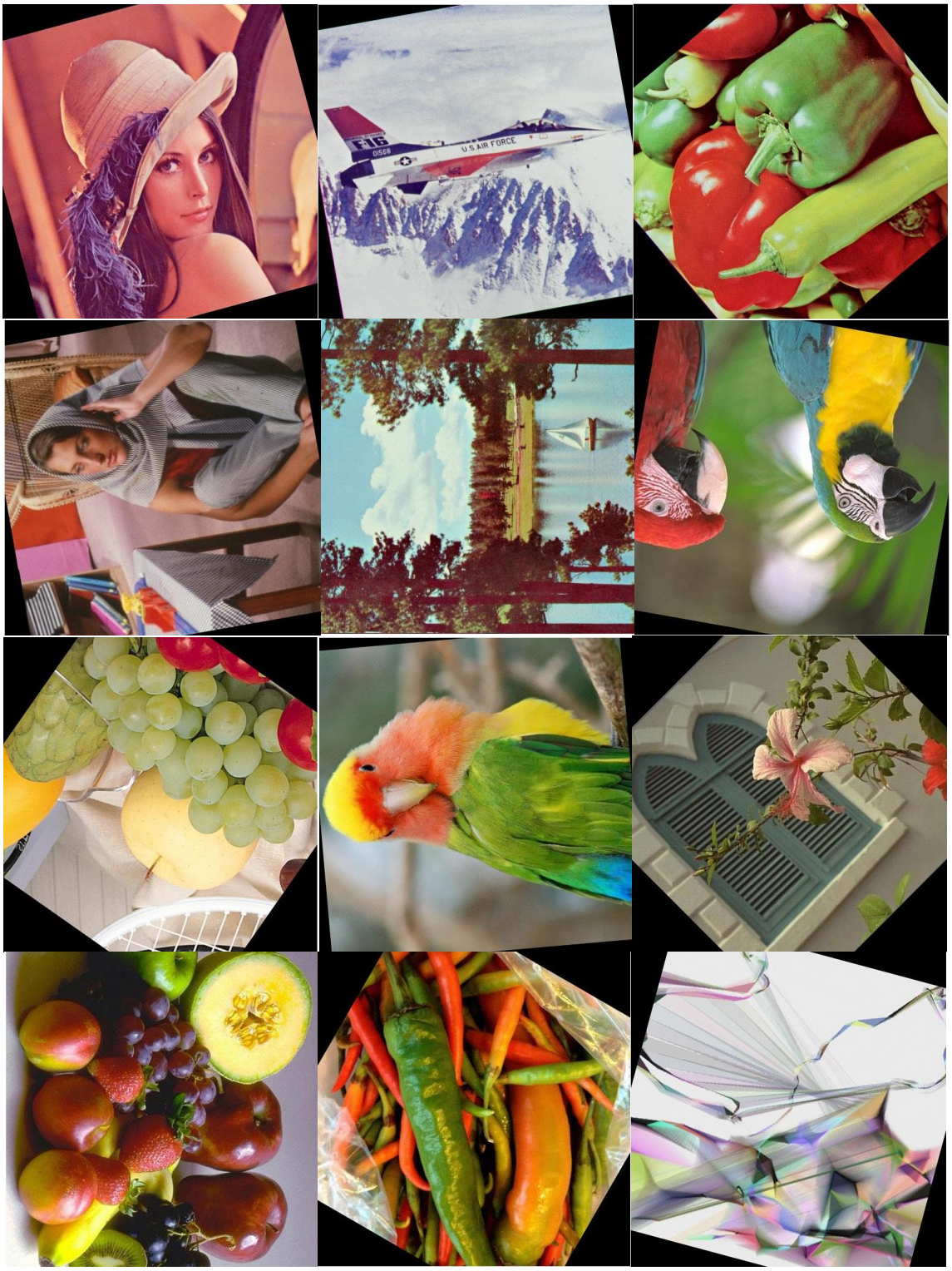
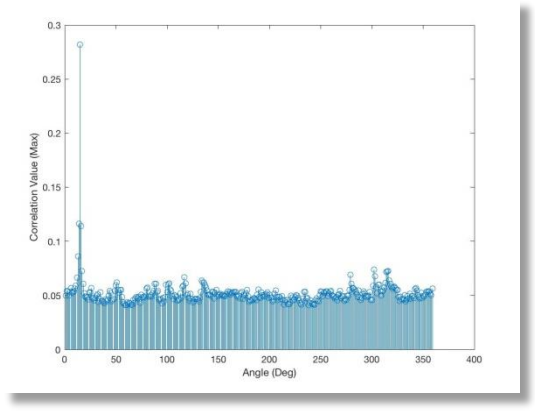
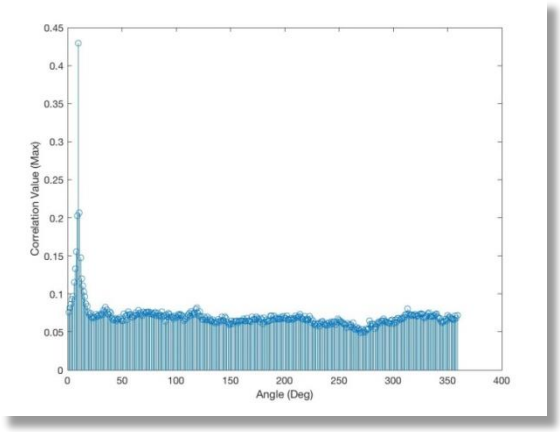


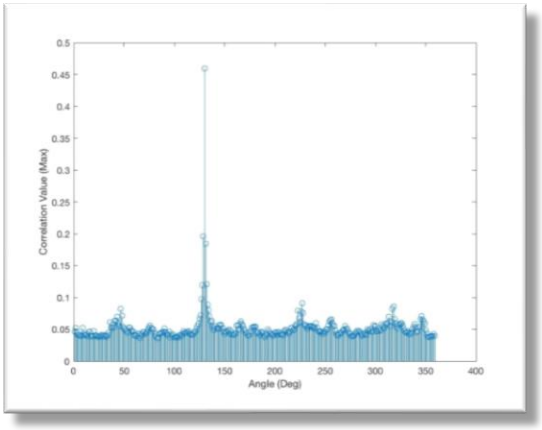
Figure 40 Rotation attack examples for different images: Lena (15^{o}), Airplane (10^{o}), Pepper (130^{o}), Barbara (100^{o}), Sailboat (90^{o}), Parrots (170^{o}), Fruits (145^{o}), Parrot (95^{o}), Flower (45^{o}), Natural (270^{o}), Pepper3 (150^{o}), Colors (345^{o}).


Correlation Value (Max)
Angle (Deg)

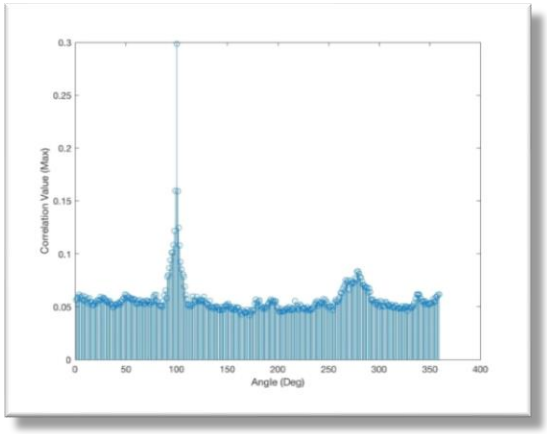
(a)


Correlation Value (Max)
Angle (Deg)

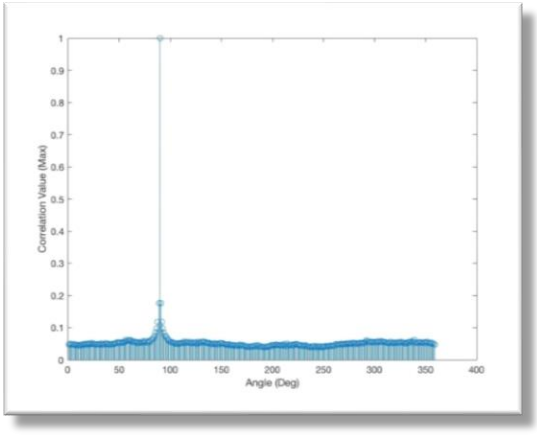
(b)


Correlation Value (Max)
Angle (Deg)

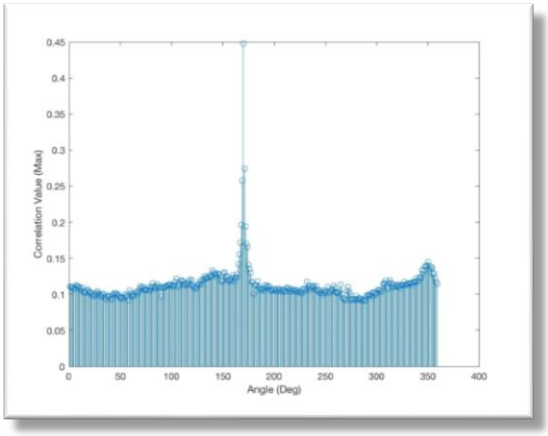
(c)


Correlation Value (Max)
Angle (Deg)

(d)


Correlation Value (Max)
Angle (Deg)

(e)


Correlation Value (Max)
Angle (Deg)

(f)

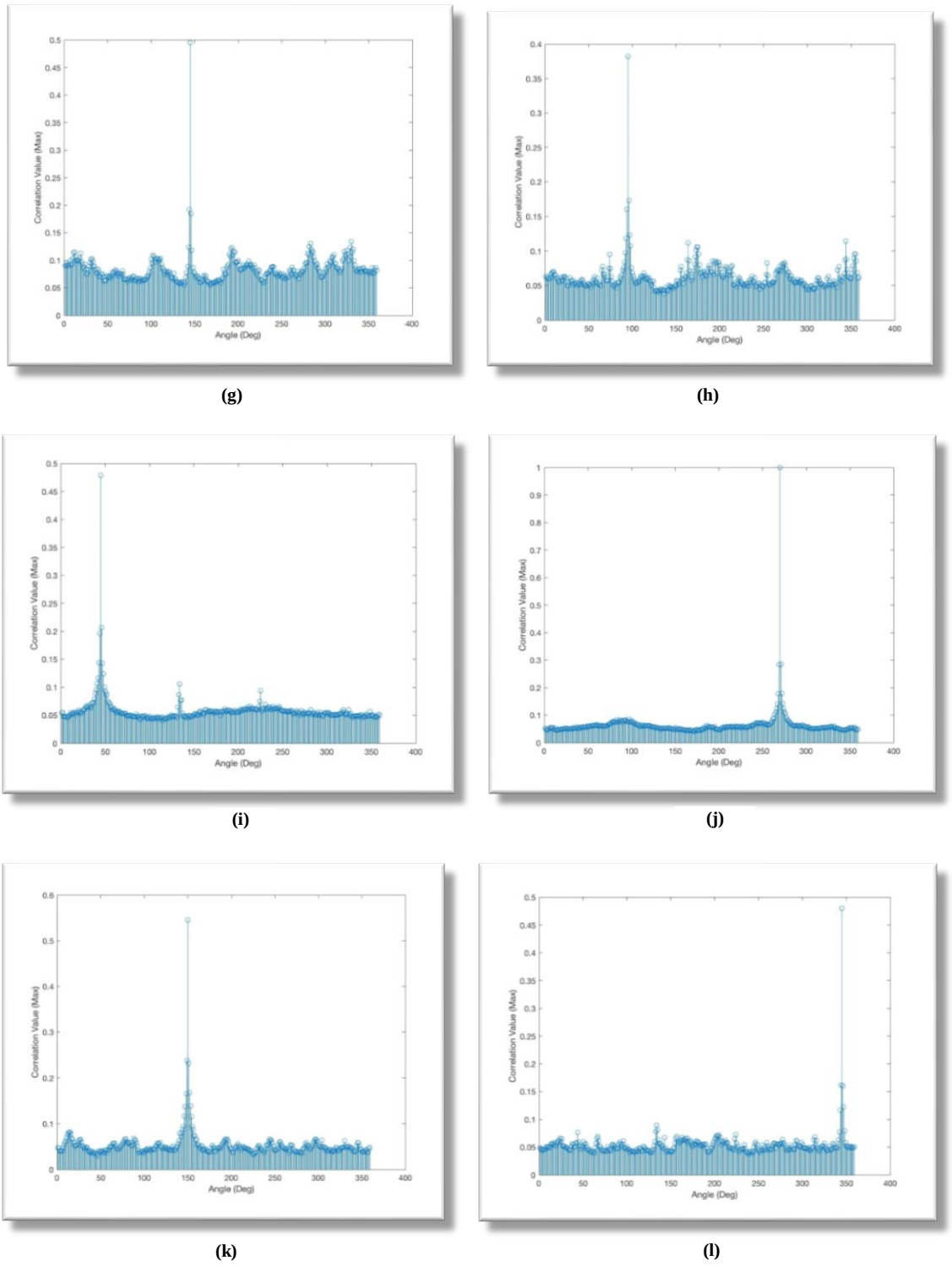


Figure 41 Normalized Cross-Correlation peaks: (a) Lena (15^o), (b) Airplane (10^o), (c) Pepper (130^o), (d) Barbara (100^o), (e) Sailboat (90^o), (f) Parrots (170^o), (g) Fruits (145^o), (h) Parrot (95^o), (i) Flower (45^o), (j) Natural (270^o), (k) Pepper3 (150^o), (l) Colors (345^o).

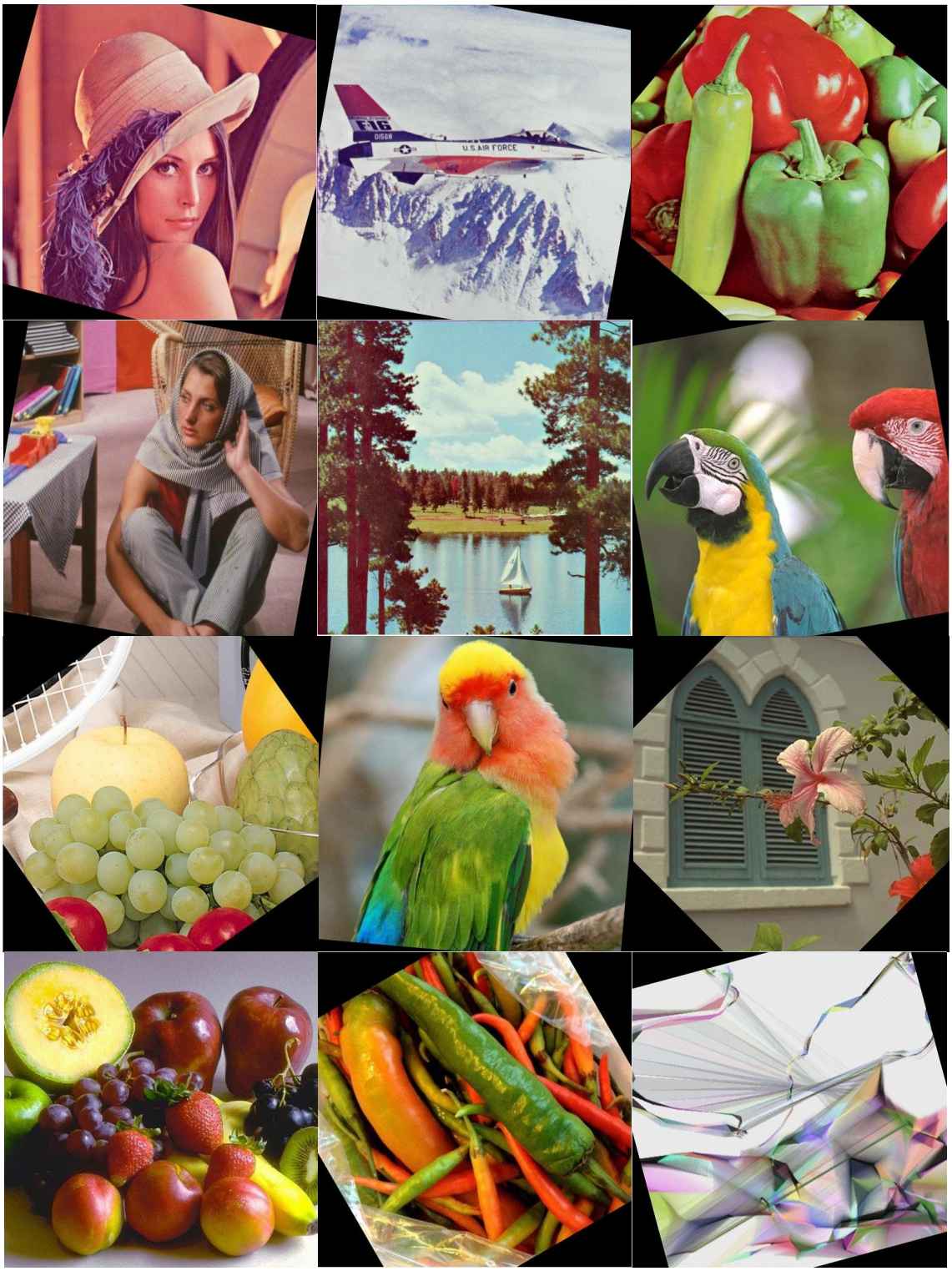
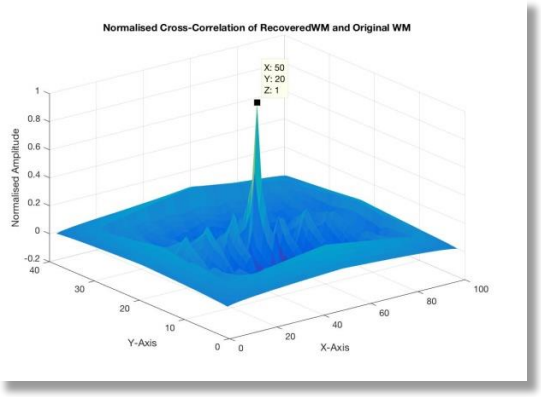
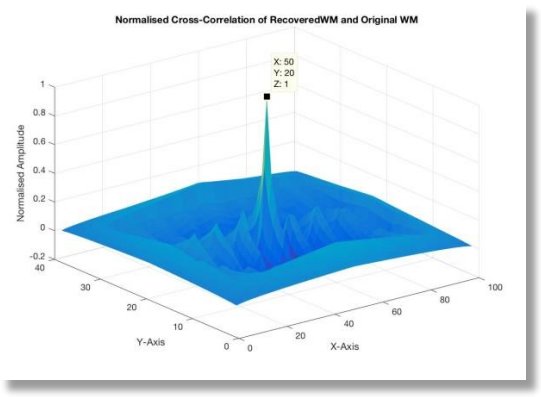


Figure 42 Restored watermarked images after undergoing a Rotation attack: Lena (-15^{o}), Airplane (-10^{o}), Pepper (-130^{o}), Barbara (-100^{o}), Sailboat (-90^{o}), Parrots (-170^{o}), Fruits (-145^{o}), Parrot (-95^{o}), Flower (-45^{o}), Natural (-270^{o}), Pepper3 (-150^{o}), Colors (-345^{o}).

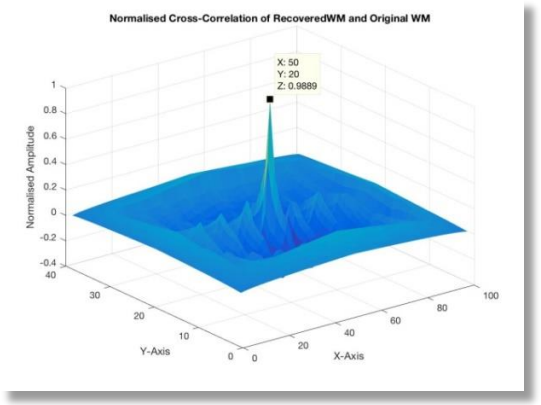
Figure 43 shows NCC values after recovering the logo from the restored images shown in Figure 43. The logo was embedded using the Cardbal2 multiwavelet. It can be seen from Figure 43 that most of the NCC values reach a value of '1' with the lowest value being '0.98' which is obtained for 'Pepper' image when rotated by 130°. The bit error rates corresponding to the NCC values in Figure 43 are shown in Table 6.



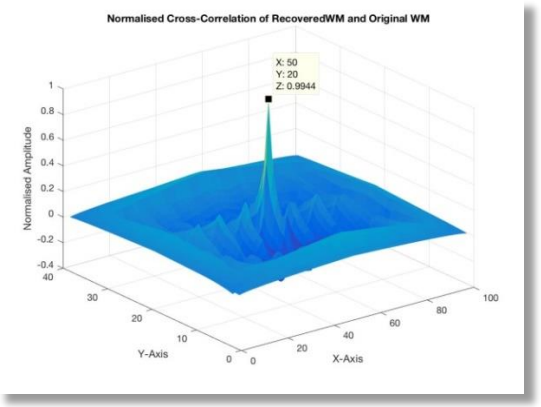
(a)



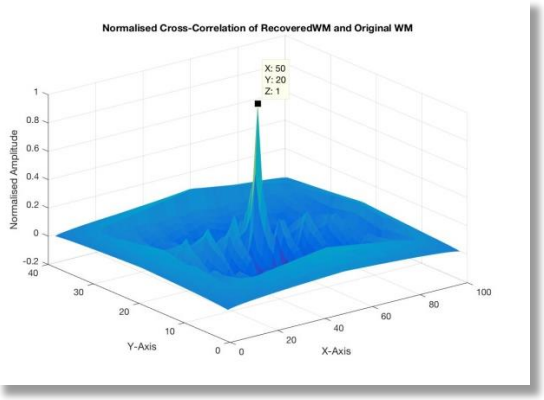
(b)



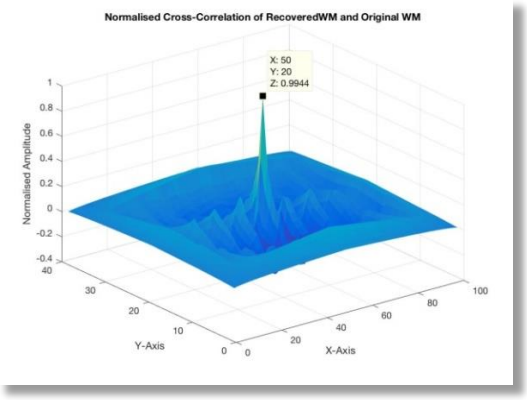
(c)



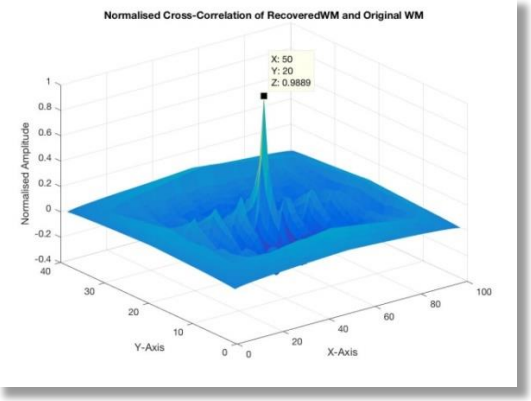
(d)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

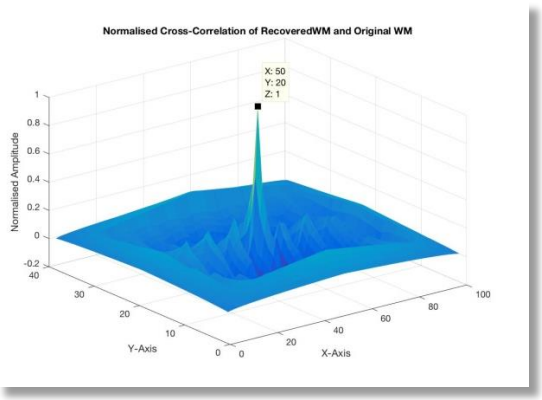
(e)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 0.9944
Normalised Amplitude
Y-Axis
X-Axis

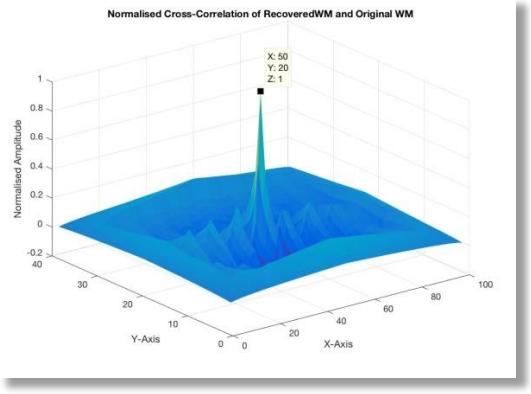
(f)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 0.9889
Normalised Amplitude
Y-Axis
X-Axis

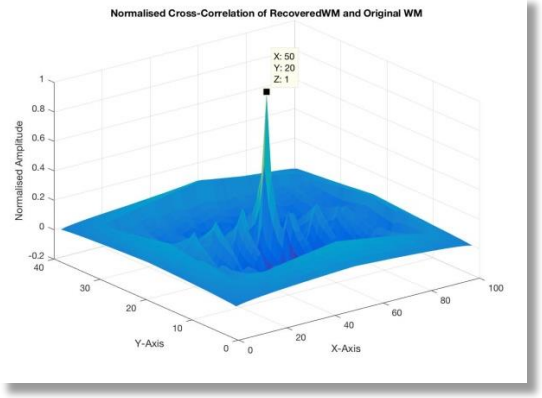
(g)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

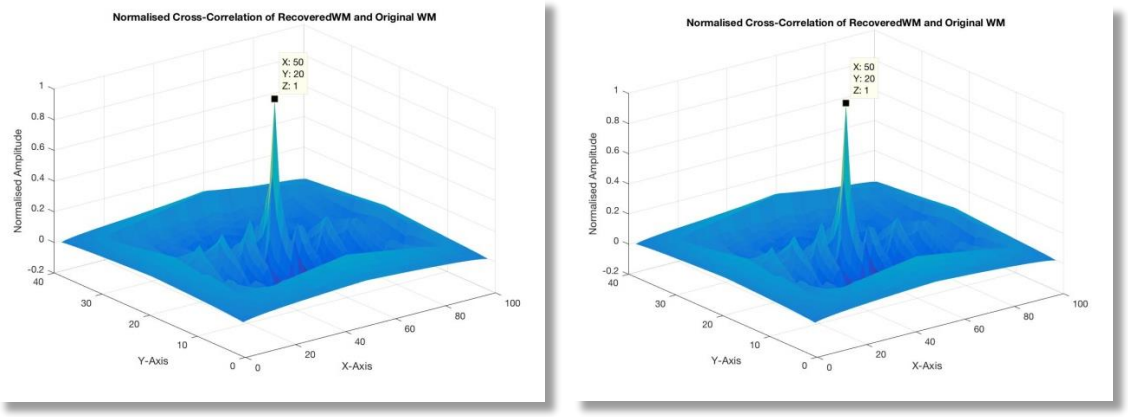
(h)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

(i)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

(j)



(k) **(l)**

Figure 43 Normalized Cross-correlation (NCC) results between the recovered and the original logos after a rotation attack: (a) Lena (15^o), (b) Airplane (10^o), (c) Pepper (130^o), (d) Barbara (100^o), (e) Sailboat (90^o), (f) Parrots (170^o), (g) Fruits (14^o), (h) Parrot (95^o), (i) Flower (45^o), (j) Natural (270^o), (k) Pepper3 (150^o), (l) Colors (345^o).

Table 6 Bit error rates corresponding to the NCC values in Figure 43.

Image	Distortion (Rotation degree)	Bit Error Rate (BER)
Lena	15^o	0
Airplane	10^o	0
Pepper	130^o	0.002
Barbara	100^o	0.001
Sailboat	90^o	0
Parrots	170^o	0.001
Fruits	145^o	0.002
Parrot2	95^o	0
Flower	45^o	0
Natural	270^o	0
Pepper3	150^o	0
Colors	345^o	0

The results for the smaller images of size 256x256 are presented next. The ‘TEST’ logo was used in these tests. Figure 44 shows the watermarked images attacked by different degrees of rotation.

Figure 44 Watermarked images of size 256x256 after rotation attacks: Lena (90^o), Pepper2 (350^o), Foods (10^o).

Figure 45 shows the detected attack parameters for each image. As it can be seen from Figure 45, the 1-bit watermark embedded in the WTMM coefficients remains robust and can be successfully used to correctly detect the attack parameters even when using smaller sized images.

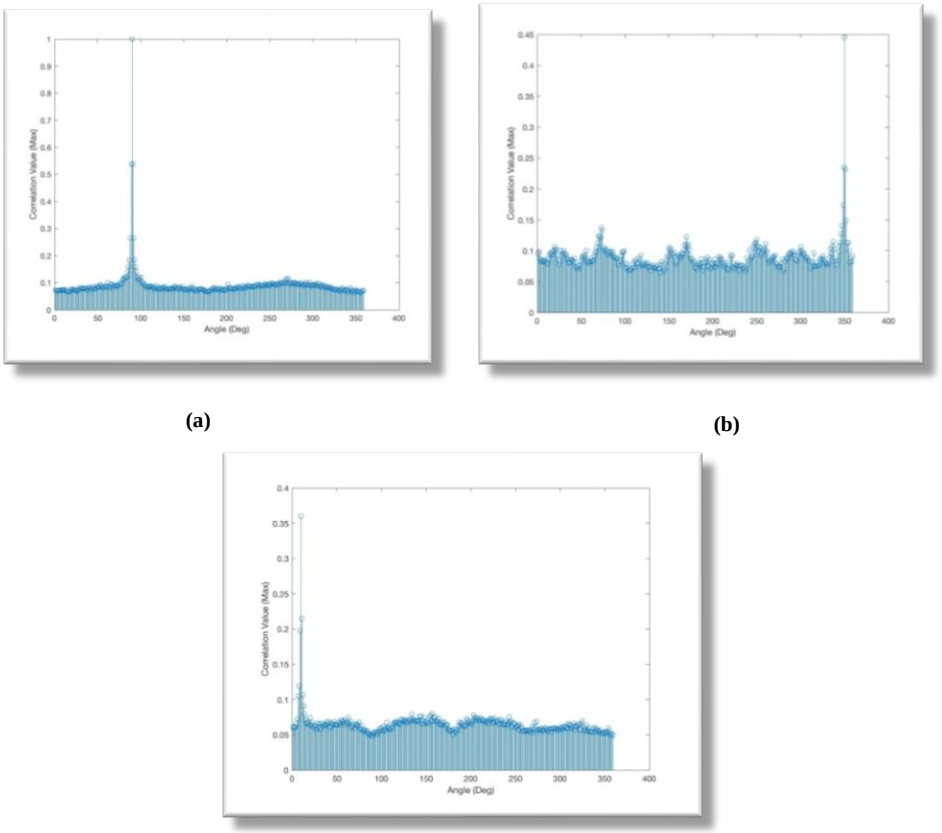


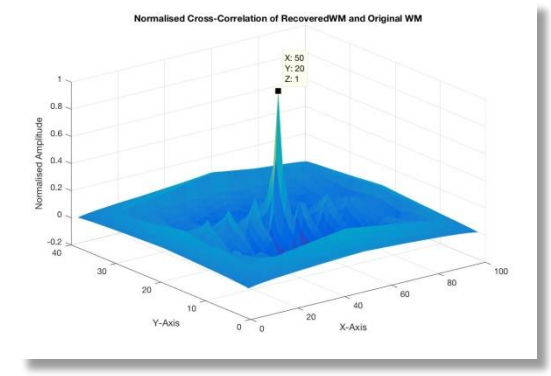
Figure 45 Normalized Cross-Correlation peaks: (a) Lena (90^o), (b) Pepper2 (350^o), (c) Foods (10^o).

Figure 46 shows the restored watermarked images once the geometric attack has been undone.

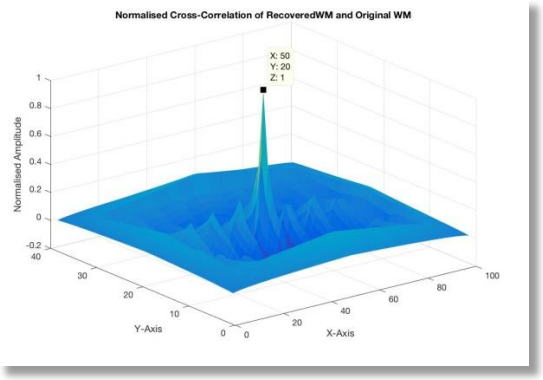
Figure 46 Restored watermarked images after undoing the rotation attacks: Lena (-90^{o}), Pepper2 (-350^{o}), Foods (-10^{o}).

Figure 47 shows the NCC values after recovering the logo from the watermarked images presented in Figure 46. The bit error rates corresponding to the NCC values in Figure 47 are shown in Table 7.

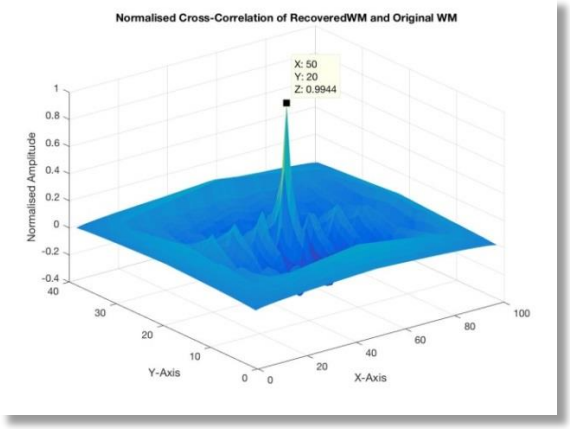
As the results presented in Figure 47 indicate, the logo watermark can still be successfully recovered.



(a)



(b)



(c)

Figure 47 Normalized Cross-Correlation (NCC) results between the recovered and the original logos after rotation attack: (a) Lena (90^o), (b) Pepper2 (350^o), (c) Foods (10^o).

Table 7 Bit error rates corresponding to the NCC values in Figure 47.

Image	Distortion (Rotation degree)	Bit Error Rate (BER)
Lena	90^o	0
Pepper2	350^o	0
Foods	10^o	0.001

As the results presented in this section demonstrate, the proposed watermarking scheme can successfully withstand rotation attacks and is able to successfully detect the logo watermark even when the cover image undergoes a rotation attack.

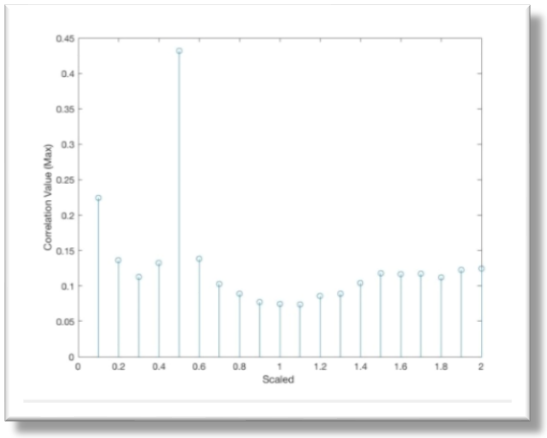
6.6.2.2 Scaling Attacks

This section presents in greater detail the experimental results for scaling attacks. Again, tests have been conducted for both 512x512 and 256x256 image sizes. As in the previous section, the logo has been embedded using the Cardbal2 multiwavelet. The interpolation method used for all scaling operations was 'bicubic' interpolation.

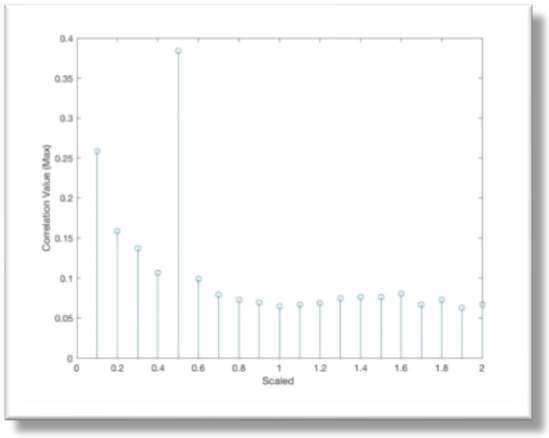
Figure 48 shows several examples of scaling attacks for various watermarked images.

Figure 48 Watermarked images after scaling attacks: Lena (0.5), Fruits (0.5), Flower (0.5), Pepper3 (0.6), Parrots (0.7), Parrot2 (0.7), Airplane (0.8), Natural (0.8), Colors (0.8), Barbara (0.9), Sailboat (0.85), Pepper (1.25).

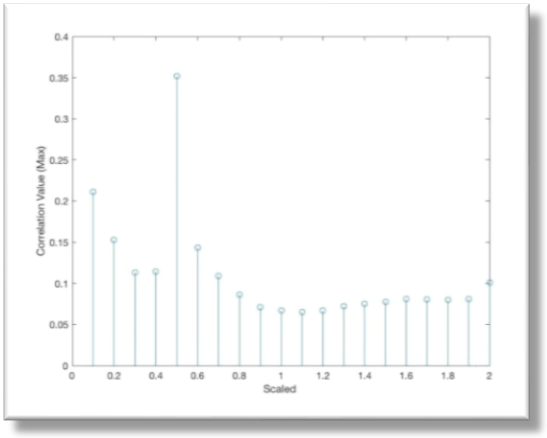
Figure 49 shows the corresponding cross-correlation peaks obtained as a result of applying Stage 1.5 of the proposed scheme. The detection of the correct amount of scaling can be carried out by performing a number of cross-correlations starting from the lowest scale to the highest scale using a certain scale step such as ‘0.1’ or even ‘0.01’ depending on the speed and level of granularity required. As it can be seen from Figure 49, the proposed Stage 1.5 algorithm can successfully detect the correct amount of scaling used for these attacks.



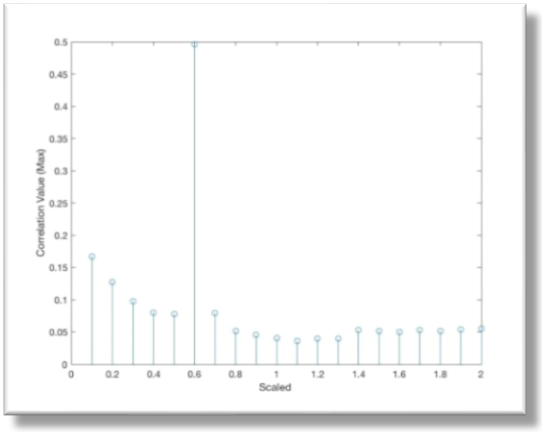
(a)



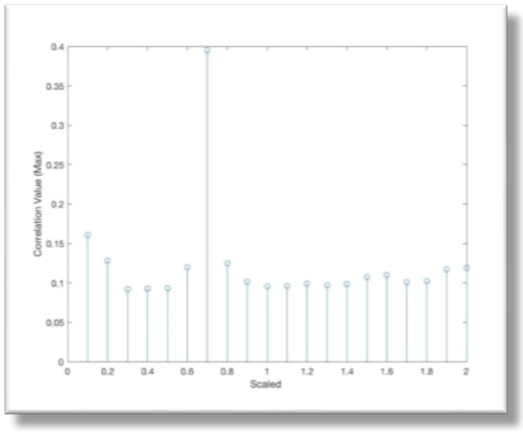
(b)



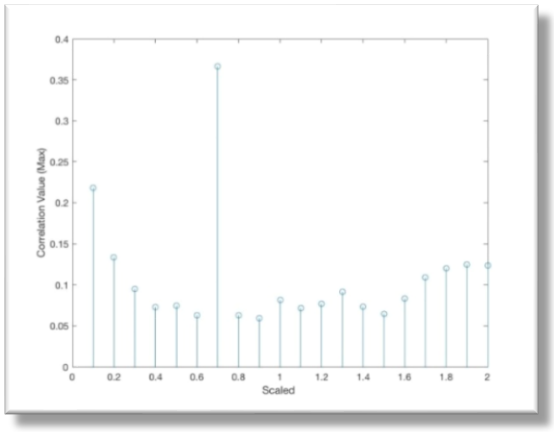
(c)



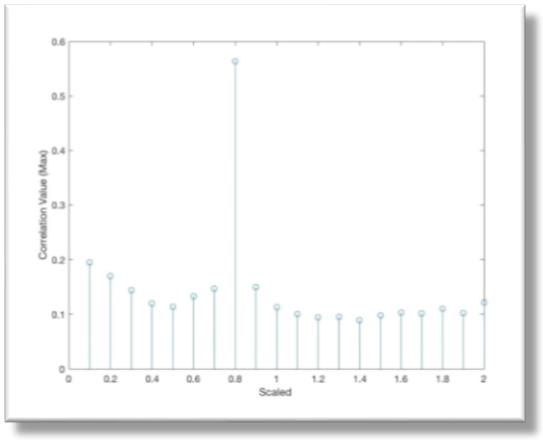
(d)


Correlation Value (Max)
Scaled

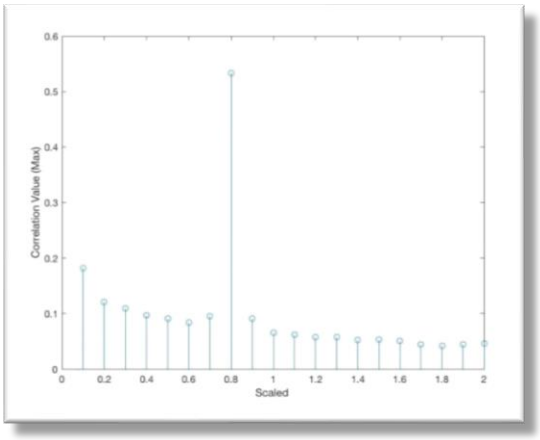
(e)


Correlation Value (Max)
Scaled

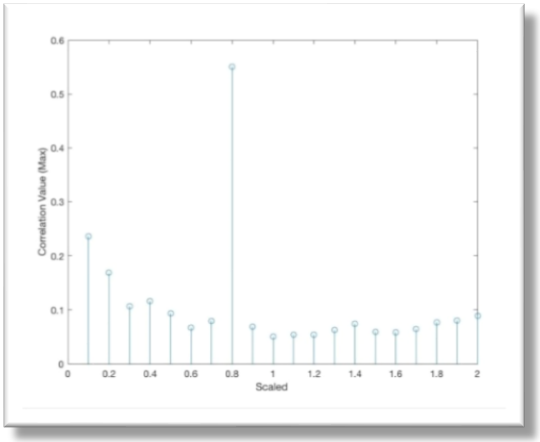
(f)


Correlation Value (Max)
Scaled

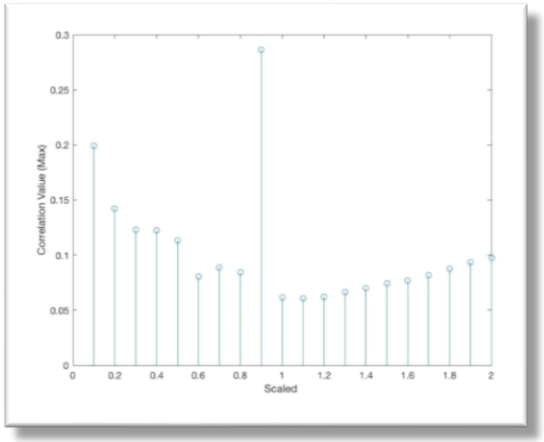
(g)


Correlation Value (Max)
Scaled

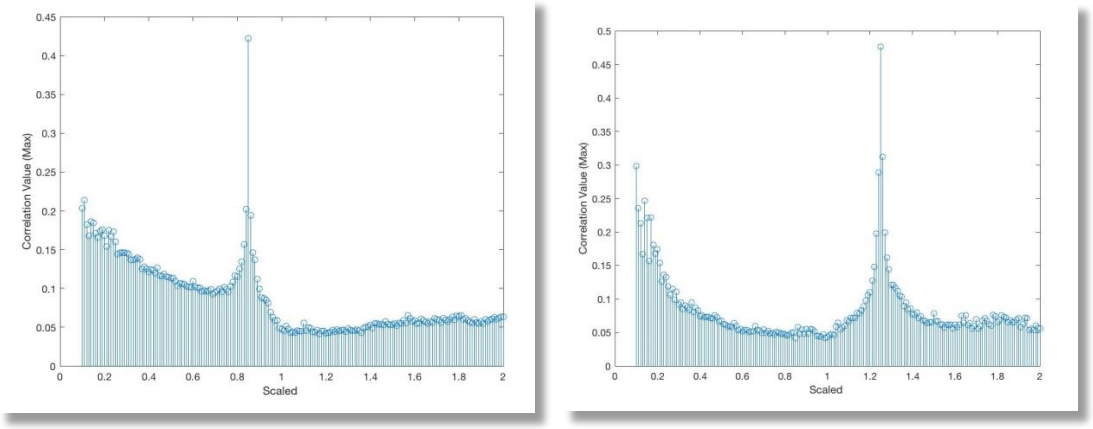
(h)


Correlation Value (Max)
Scaled

(i)


Correlation Value (Max)
Scaled

(j)



(k) **(l)**

Figure 49 Normalized Cross-Correlation peaks: (a) Lena (0.5), (b) Fruits (0.5), (c) Flower (0.5), (d) Pepper3 (0.6), (e) Parrots (0.7), (f) Parrot2 (0.7), (g) Airplane (0.8), (h) Natural (0.8), (i) Colors (0.8), (j) Barbara (0.9), (k) Sailboat (0.85), (l) Pepper (1.25).

Figure 50 shows the restored watermarked images after undoing the attack using the detected parameters shown in Figure 49.

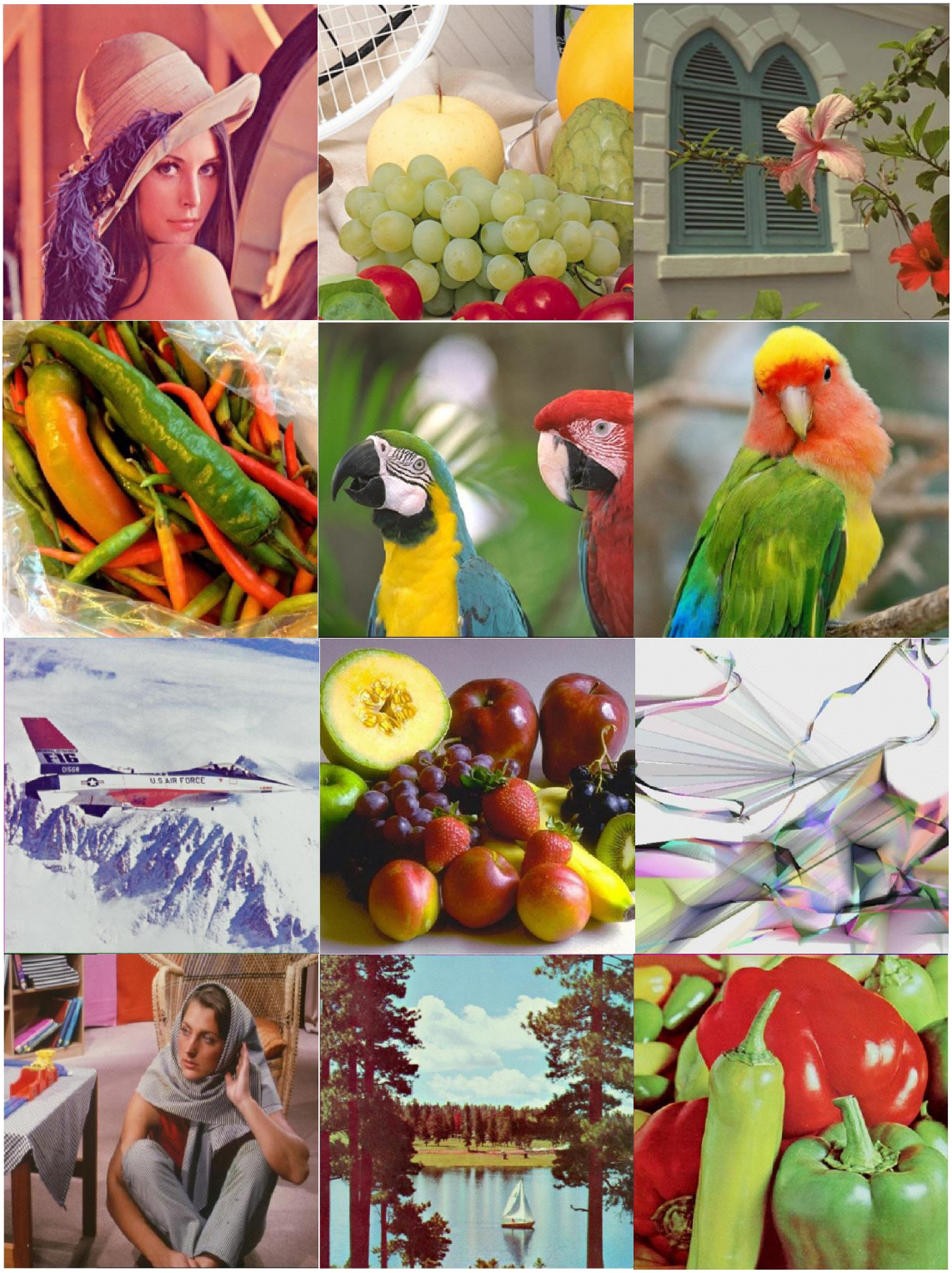
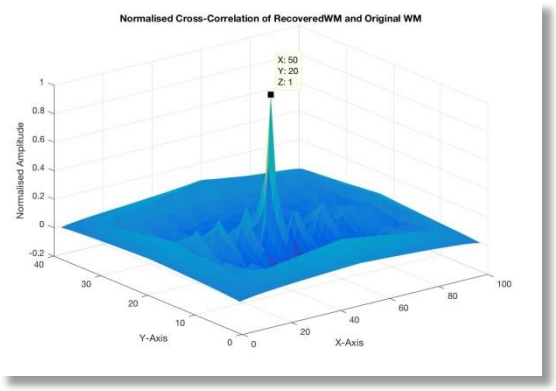
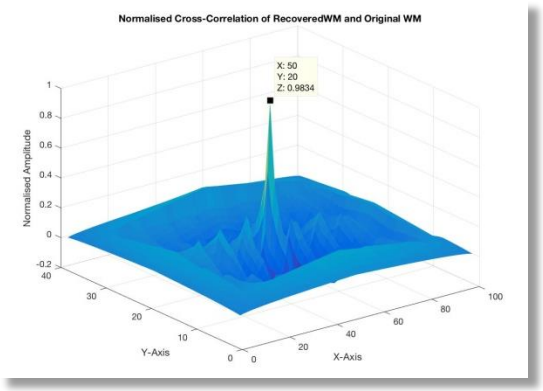


Figure 50 Restored watermarked images after undoing the scaling attacks: Lena, Fruits, Flower, Pepper3, Parrots, Parrot2, Airplane, Natural, Colors, Barbara, Sailboat, Pepper.

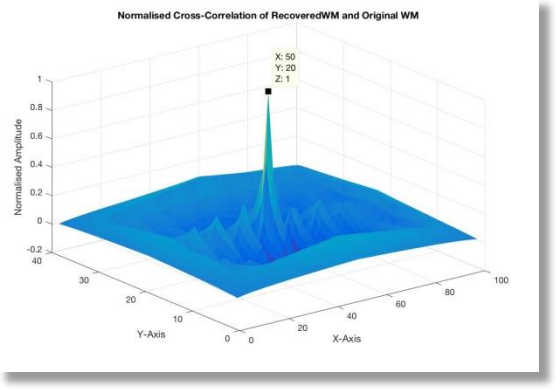
Figure 51 shows the NCC values for the recovered logo watermark. It can be seen from the figures that most of the recovered logos achieve an NCC value of '1'. The lowest NCC value (0.98) is obtained for the 'Fruits' image when scaled by a factor of 0.5. Hence, overall, all the logos are successfully recovered. The bit error rates corresponding to the NCC values in Figure 51 are shown in Table 8.



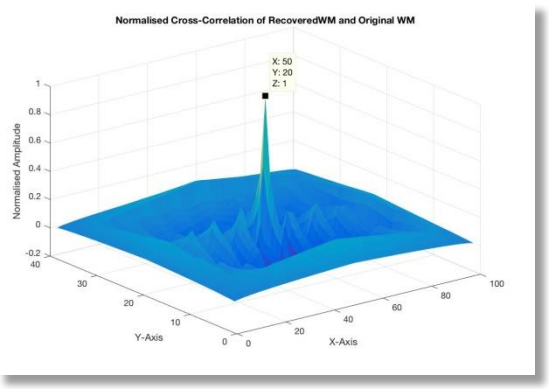
(a)



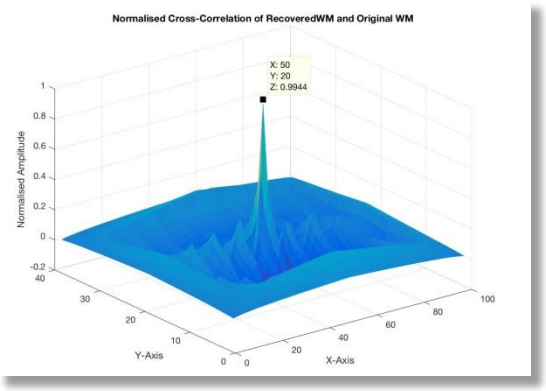
(b)



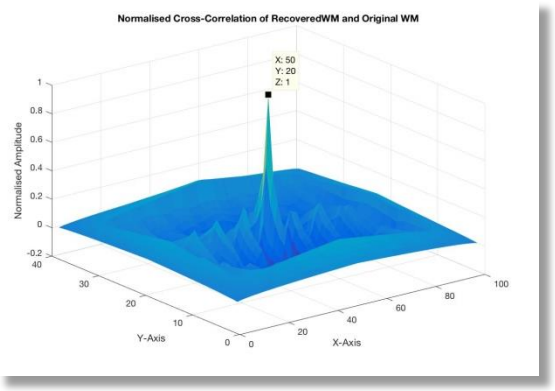
(c)



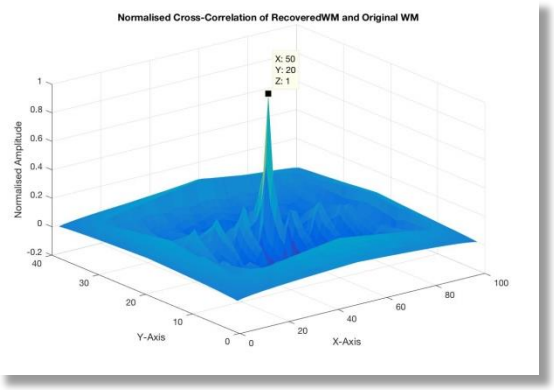
(d)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 0.9944
Normalised Amplitude
Y-Axis
X-Axis

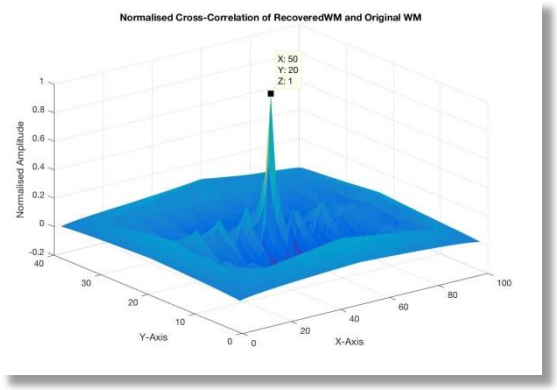
(e)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

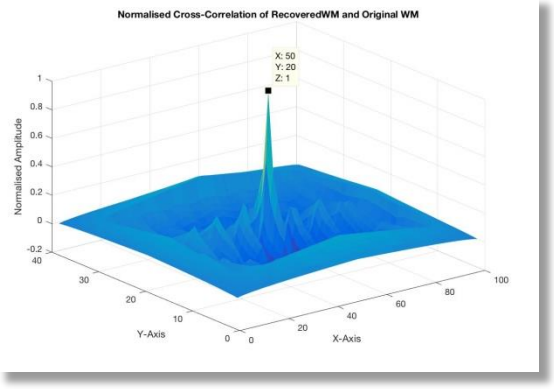
(f)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

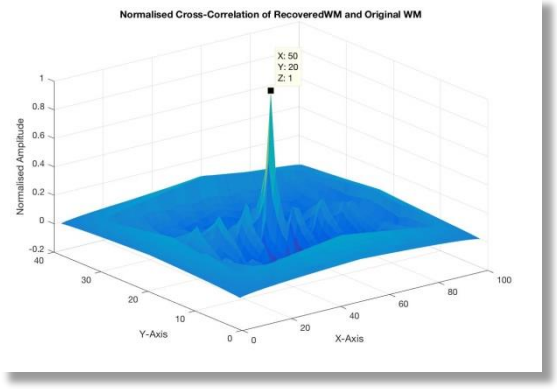
(g)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

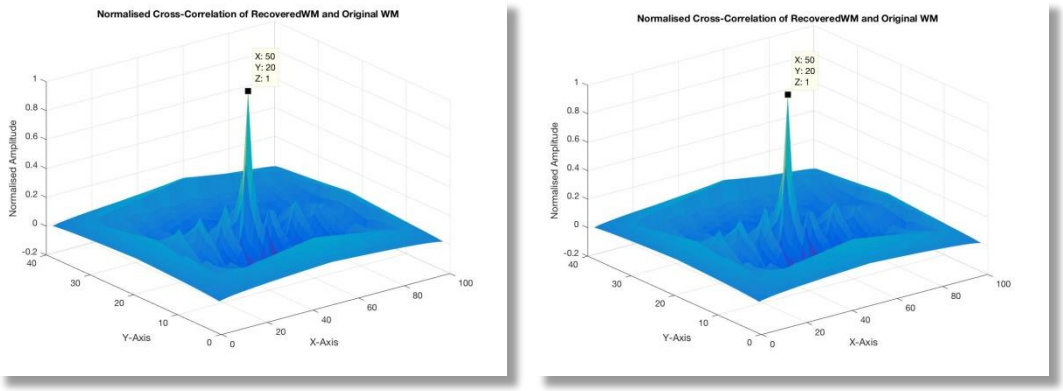
(h)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

(i)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

(j)



(k) **(l)**

Figure 51 (a) Lena (0.5), (b) Fruits (0.5), (c) Flower (0.5), (d) Pepper3 (0.6), (e) Parrots (0.7), (f) Parrot2 (0.7), (g) Airplane (0.8), (h) Natural (0.8), (i) Colors (0.8), (j) Barbara (0.9), (k) Sailboat (0.85), (l) Pepper (1.25).

Table 8 Bit error rates corresponding to the NCC values in Figure 51.

Image	Distortion (Scaling Factor)	Bit Error Rate (BER)
Lena	0.5	0
Fruits	0.5	0.003
Flower	0.5	0
Pepper3	0.6	0
Parrots	0.7	0.001
Parrot2	0.7	0
Airplane	0.8	0
Natural	0.8	0
Colors	0.8	0
Barbara	0.9	0
Sailboat	0.85	0
Pepper	1.25	0

The results for 256x256 size images are presented next. Figure 52 shows some scaling attack examples for smaller 256x256 images.

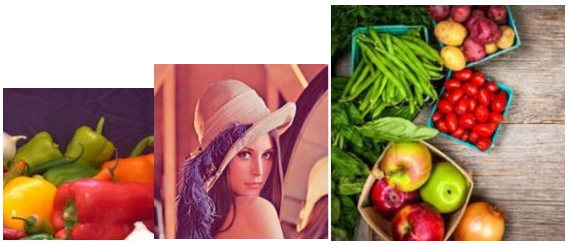
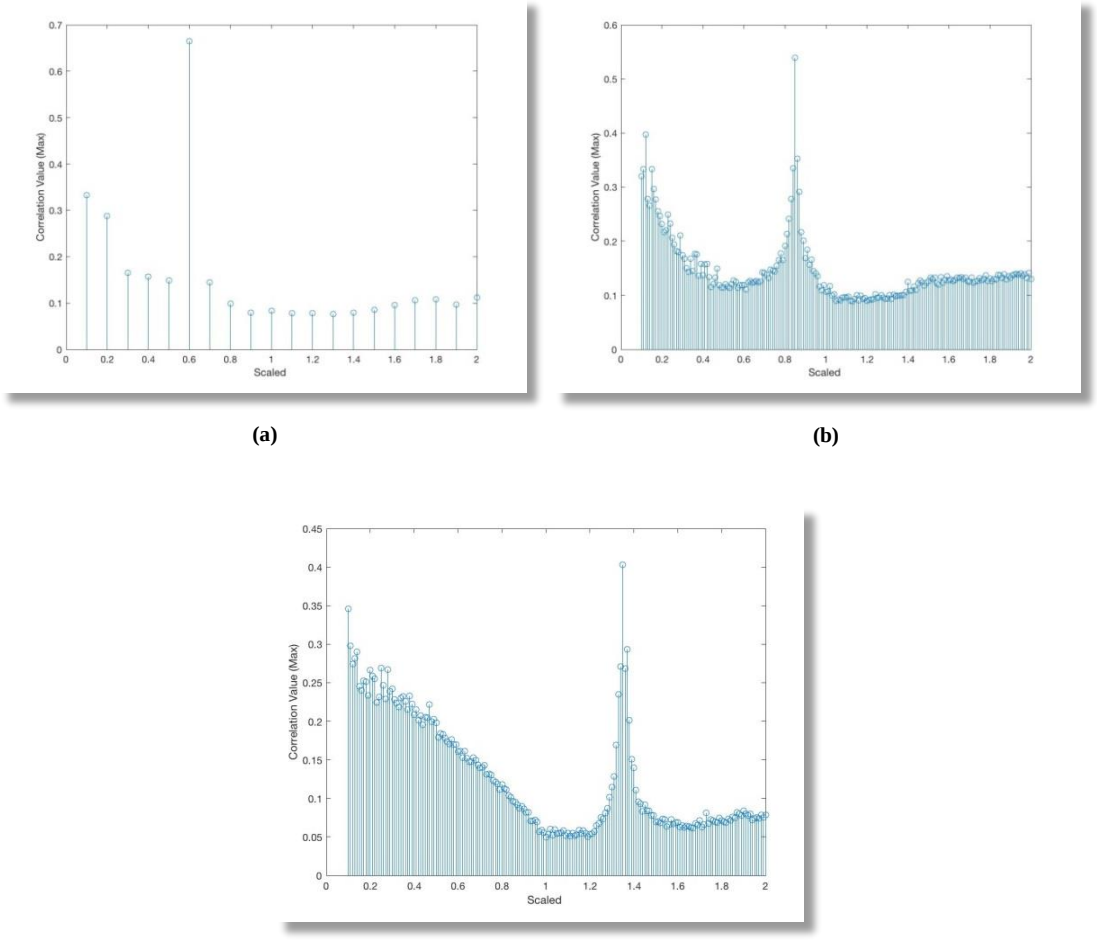


Figure 52 Watermarked images of size 256x256 after scaling attacks: Pepper2 (0.6), Lena (0.85), Foods (1.35).

As it can be seen from Figure 53, the scaling attack parameters can still be successfully detected but predictably, the margins between the cross-correlation peaks are now lower.



(a) **(b)**

(c)

Figure 53 Normalized Cross-Correlation peaks: (a) Pepper2 (0.6), (b) Lena (0.85), (c) Foods (1.35).

Figure 54 shows the restored watermarked images after the geometric attack has been undone according to the identified attack parameters presented in Figure 53.

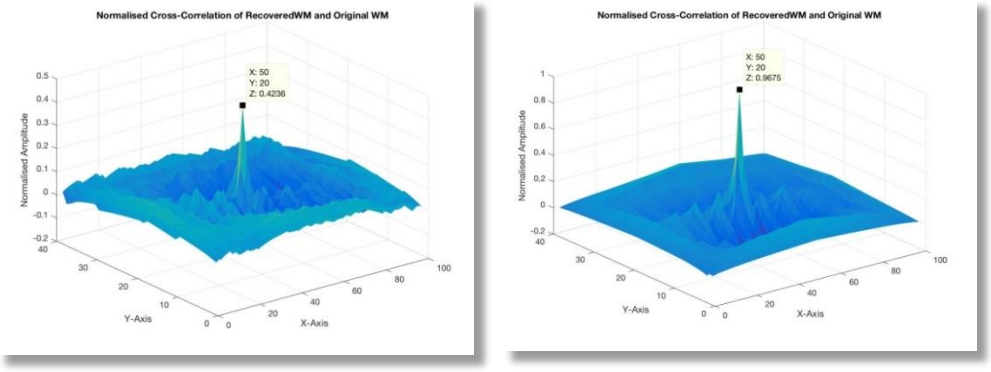
Figure 54 Restored watermarked images after undergoing a scaling attack: Pepper2, Lena, Foods.

The normalized cross-correlation results obtained after recovering the logo watermark after undoing the attack are shown in Figure 56. As it can be seen from the figure, the first three images pose no problems, but in the case of the last image which has been subjected to a stronger attack, the NCC is only 0.42. The recovered logo in this case is shown in Figure 55.

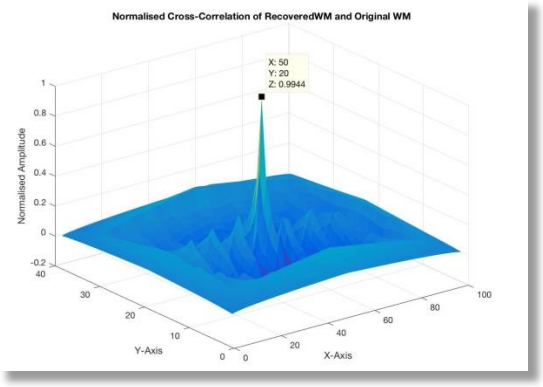
(a) **(b)**

Figure 55 The recovered 'TEST' logo watermark: (a) The original logo watermark, and (b) the recovered logo watermark for the 'Pepper2' image after undergoing a scaling attack (Scaling: 0.6; NCC: 0.42).

While scaling images with a factor higher than 1.00 causes no issues, for more aggressive scaling factors (below 1.00), the NCC values start to decrease. This is because the resulting size of the watermarked image after attack becomes too small and by implication the chip rate becomes too small to be able to reliably carry a logo of this size. The bit error rates corresponding to the NCC values in Figure 56 are shown in Table 9.



(a) **(b)**



(c)

Figure 56 Normalized Cross-Correlation (NCC) results between the recovered and the original logos after recovering the logo from a scaling attack for 256x265 images: (a) Pepper2 (0.6), (b) Lena (0.85), (c) Foods 1.35).

The results in Figure 48 – Figure 56 demonstrate that the proposed watermarking scheme can successfully detect and recover a watermark even if the cover image undergoes a scaling attack and even for 256x256 images as long as the attack remains in reasonable limits. Larger 512x512 images are robust enough to withstand any 'normal' scaling attack.

Table 9 Bit error rates corresponding to the NCC values in Figure 56.

Image	Distortion (Scaling Factor)	Bit Error Rate (BER)
Pepper2	0.6	0.186
Lena	0.85	0.006
Foods	1.35	0.001

6.6.2.3 Translation Attacks

This section presents in more detail the experimental results for translation attacks using images of size 512x512 and 256x256. As in previous sections, the Cardbal2 multiwavelet has been used to embed the logo. Figure 57 shows several examples of translation attacks which can shift the watermarked images both horizontally and vertically. This can be also seen as a form of cropping attack.

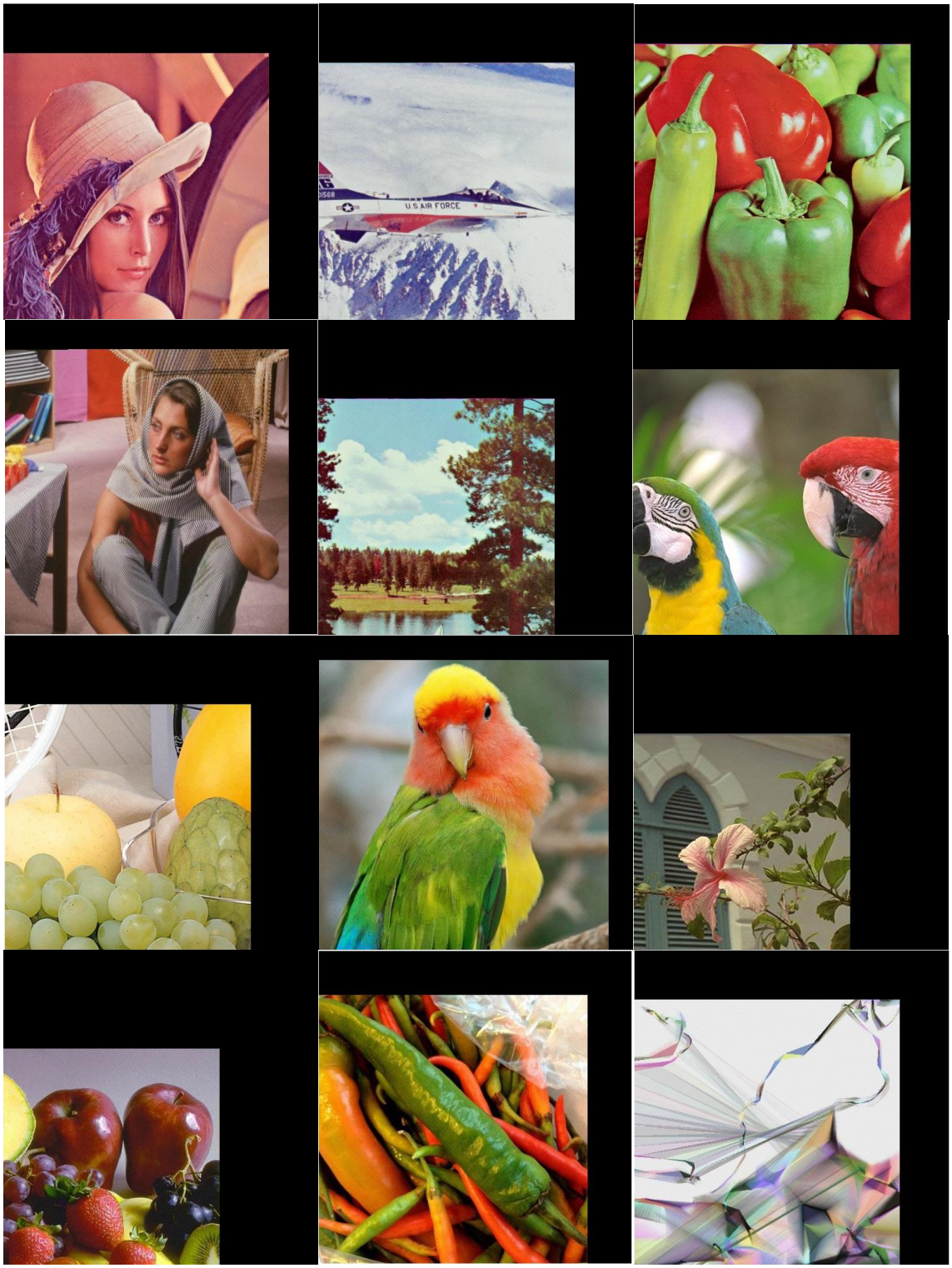
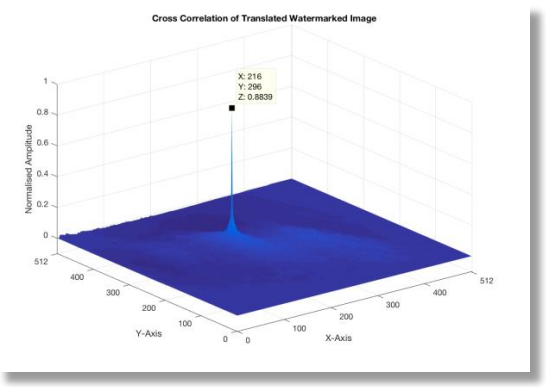
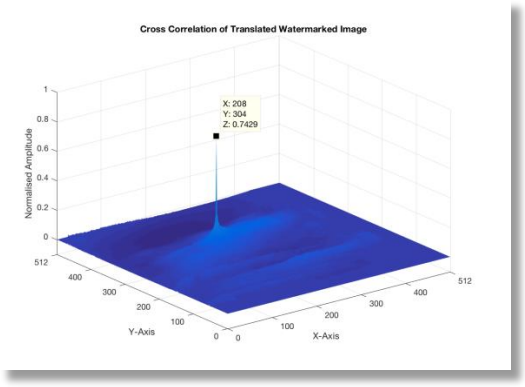


Figure 57 Watermarked images subjected to translation attacks: Lena (+80, -80), Airplane (+96, -96), Pepper (+64, -64), Barbara (+48, -48), Sailboat (+128, -128), Parrots (+80, -80), Fruits (+112, -112), Parrot2 (+40, -40), Flower (+160, -160), Natural (+160, -160), Pepper3 (+72, -72), Colors (+80, -80).

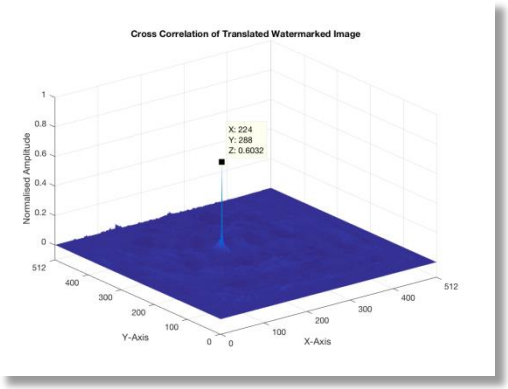
Figure 58 shows the detected attack parameters obtained as a result of applying Stage 1.5 of the proposed scheme. The attack parameters are detected with the help of cross-correlation. The location of the maximum cross-correlation peak is related to the parameters of the translation attack. This is shown in Figure 58 where the 'X' and 'Y' represent the x and y coordinates of the peak value in the cross-correlation matrix while 'Z' represents the magnitude of the normalised cross-correlation peak. The exact parameters of the translation attack are found by subtracting the height and width of the WTMM image from the values 'X' and 'Y' respectively.



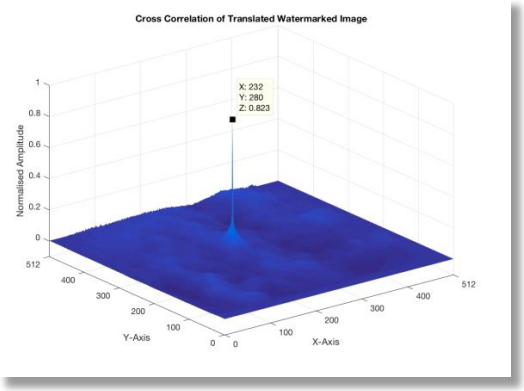
(a)



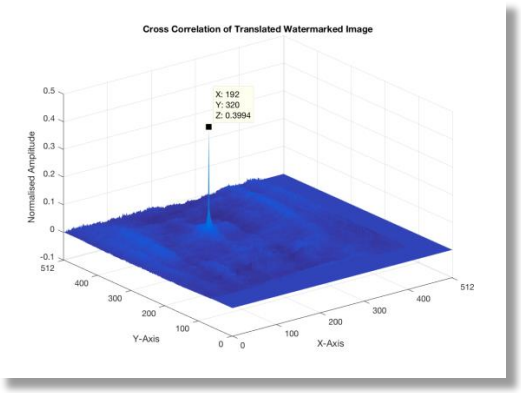
(b)



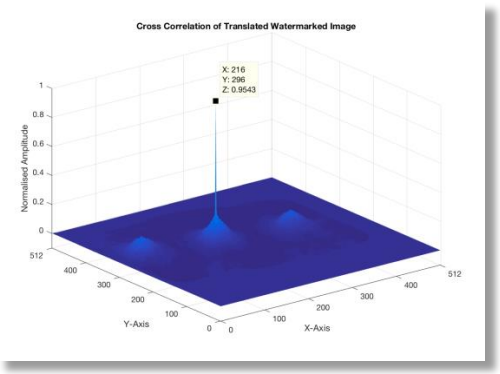
(c)



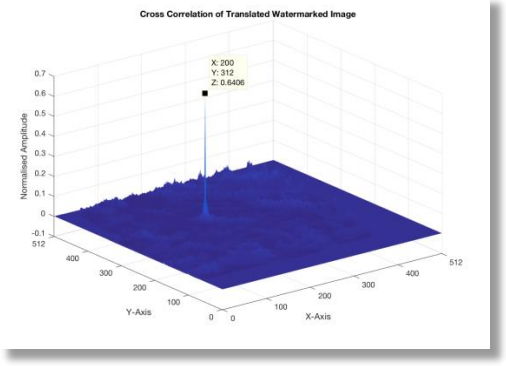
(d)


Cross Correlation of Translated Watermarked Image
X: 192
Y: 320
Z: 0.3994
Normalised Amplitude
Y-Axis
X-Axis

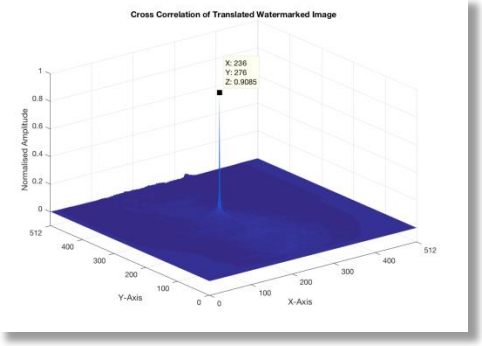
(e)


Cross Correlation of Translated Watermarked Image
X: 216
Y: 296
Z: 0.9543
Normalised Amplitude
Y-Axis
X-Axis

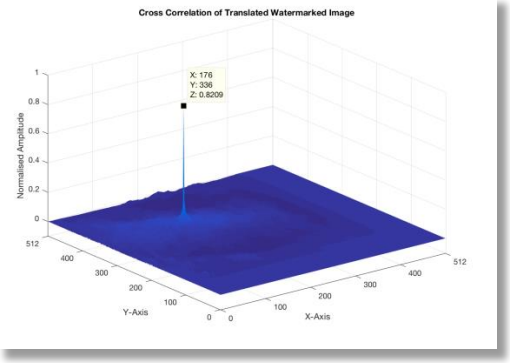
(f)


Cross Correlation of Translated Watermarked Image
X: 200
Y: 312
Z: 0.6406
Normalised Amplitude
Y-Axis
X-Axis

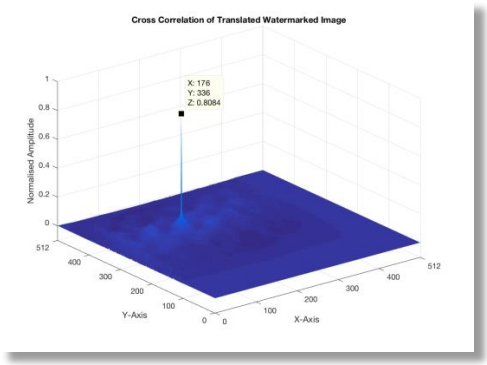
(g)


Cross Correlation of Translated Watermarked Image
X: 236
Y: 276
Z: 0.9085
Normalised Amplitude
Y-Axis
X-Axis

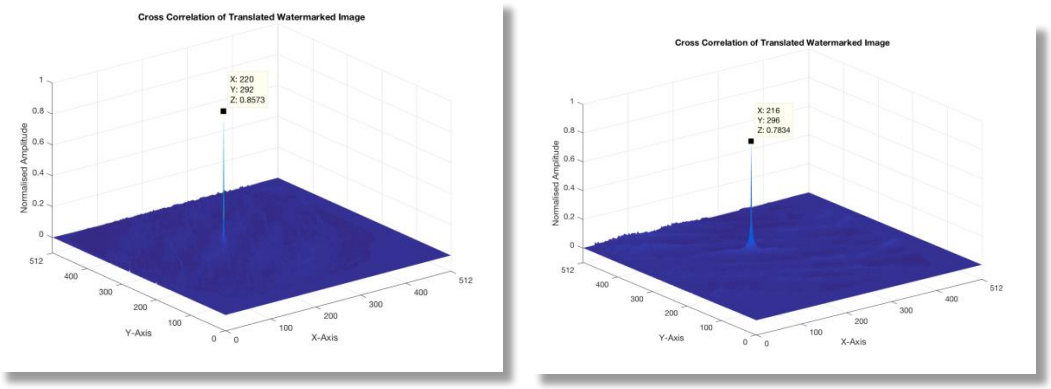
(h)


Cross Correlation of Translated Watermarked Image
X: 176
Y: 336
Z: 0.8209
Normalised Amplitude
Y-Axis
X-Axis

(i)


Cross Correlation of Translated Watermarked Image
X: 176
Y: 336
Z: 0.8084
Normalised Amplitude
Y-Axis
X-Axis

(j)



(k) **(l)**

Figure 58 Detection of translation parameters through cross correlation: (a) Lena (+80, -80), (b) Airplane (+96, -96), (c) Pepper (+64, -64), (d) Barbara (+48, -48), (e) Sailboat (+128, -128), (f) Parrots (+80, -80), (g) Fruits (+112, -112), (h) Parrot2 (+40, -40), (i) Flower (+160, -160), (j) Natural (+160, -160), (k) Pepper3 (+72, -72), (l) Colors (+80, -80).

Figure 59 shows the restored watermarked images after undoing the translation attack based on the attack parameters calculated via cross-correlation.

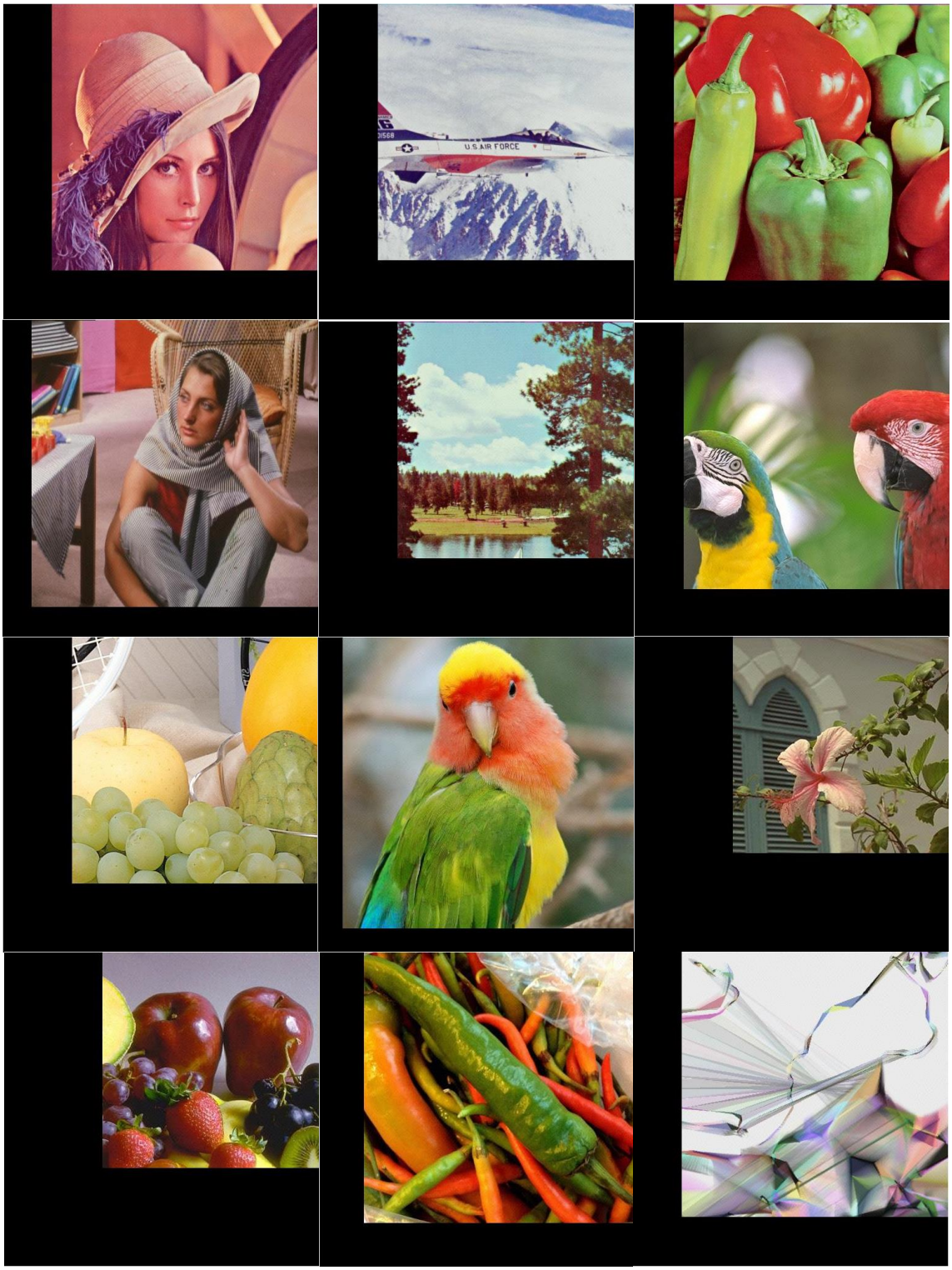
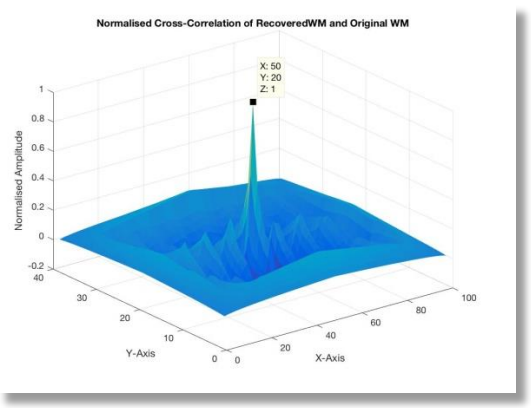
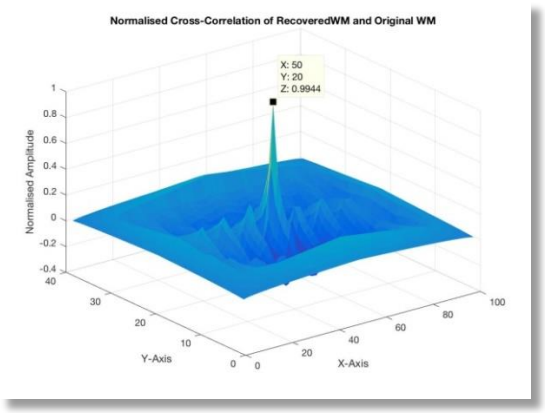


Figure 59 Restored watermarked images after undoing the translation attacks: Lena (-80, +80), Airplane (-96, +96), Pepper (-64, +64), Barbara (-48, +48), Sailboat (-128, +128), Parrots (-80, +80), Fruits (-112, +112), Parrot2 (-40, +40), Flower (-160, +160), Natural (-160, +160), Pepper3 (-72, +72), Colors (-80, +80).

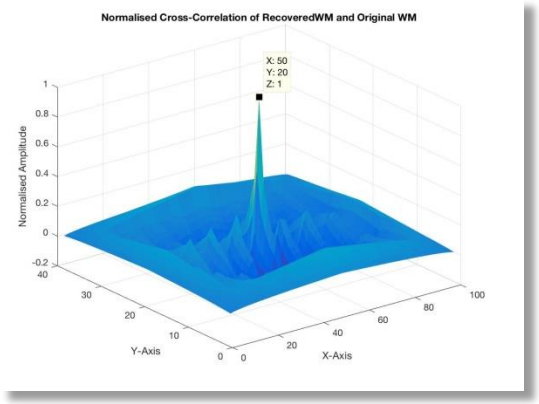
Figure 60 shows the normalized cross-correlation of the recovered logo watermark from the restored watermarked images. The lowest obtained NCC value (0.97) is for the 'flower' image which has been subjected to the highest amount of translation (160, 160) which leads to a significant loss of the original image content. The original logo watermark and the recovered logo watermark for this case are shown in Figure 61. The bit error rates corresponding to the NCC values in Figure 56 are shown in Table 10.



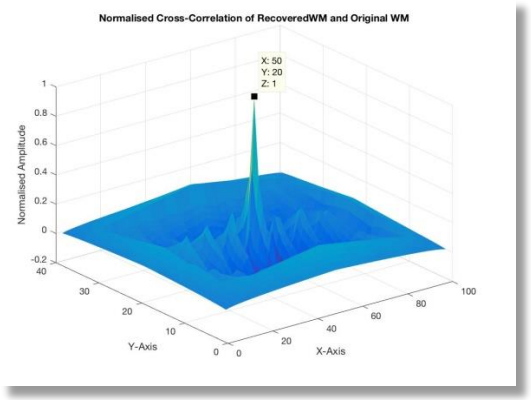
(a)



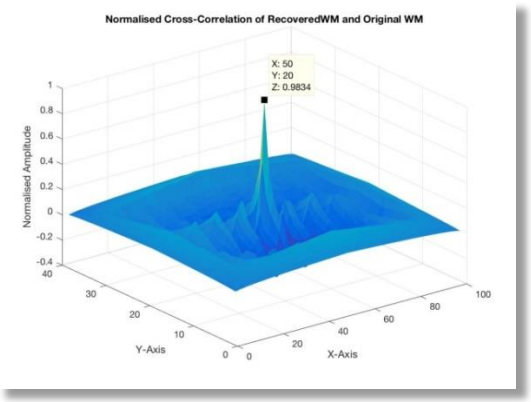
(b)



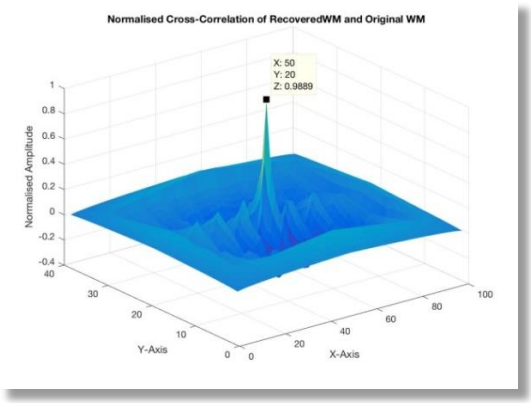
(c)



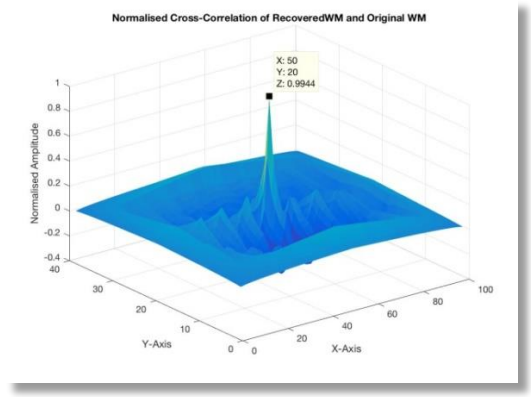
(d)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 0.9834
Normalised Amplitude
Y-Axis
X-Axis

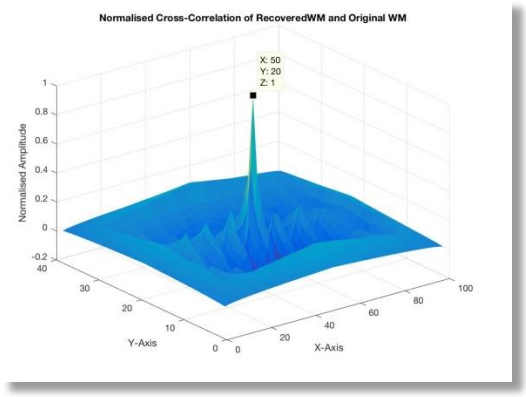
(e)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 0.9889
Normalised Amplitude
Y-Axis
X-Axis

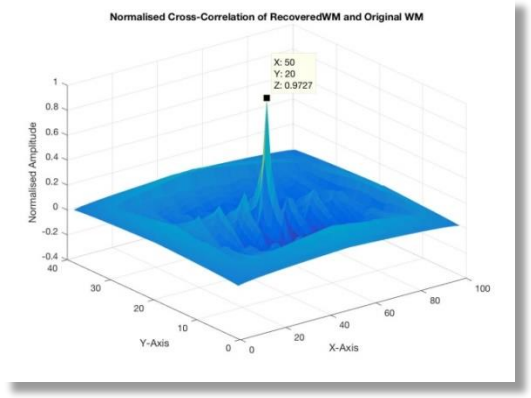
(f)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 0.9944
Normalised Amplitude
Y-Axis
X-Axis

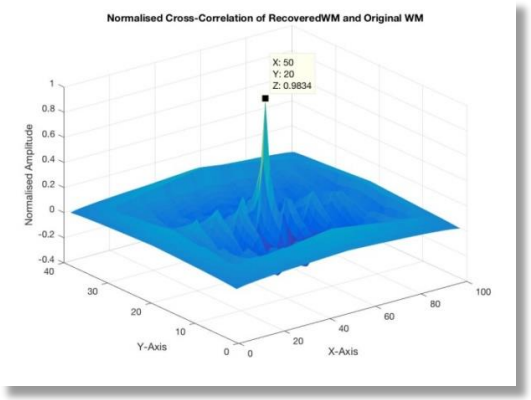
(g)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 1
Normalised Amplitude
Y-Axis
X-Axis

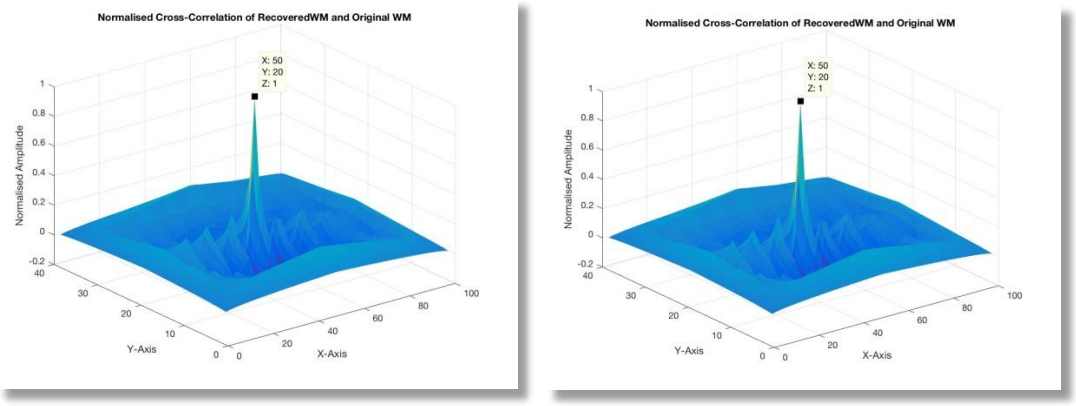
(h)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 0.9727
Normalised Amplitude
Y-Axis
X-Axis

(i)


Normalised Cross-Correlation of RecoveredWM and Original WM
X: 50
Y: 20
Z: 0.9834
Normalised Amplitude
Y-Axis
X-Axis

(j)



(k) **(l)**

Figure 60 Normalized Cross-Correlation (NCC) results between the recovered and the original logos after recovering the logo from a translation attack: (a) Lena (-80, +80), (b) Airplane (-96, +96), (c) Pepper (-64, +64), (d) Barbara (-48, +48), (e) Sailboat (-128, +128), (f) Parrots (-80, +80), (g) Fruits (-112, +112), (h) Parrot2 (-40, +40), (i) Flower (-160, +160), (j) Natural (-160, +160), (k) Pepper3 (-72, +72), (l) Colors (-80, +80).

(a) **(b)**

Figure 61 The recovered 'TEST' logo watermark: (a) The original logo watermark, and (b) the recovered logo watermark for the 'Flower' image after undergoing a translation attack (Translation: 160, 160; NCC: 0.97).

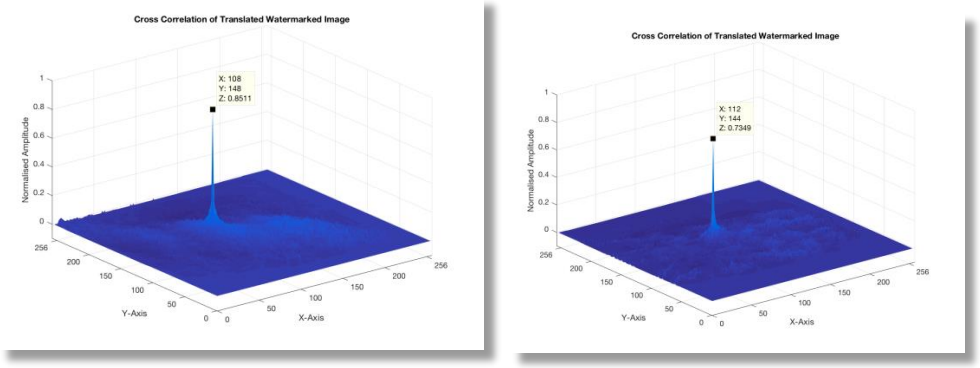
Table 10 Bit error rates corresponding to the NCC values in Figure 60.

Image	Distortion (Translation offset x, y)	Bit Error Rate (BER)
Lena	(80, 80)	0
Airplane	(96, 96)	0.001
Pepper	(64, 64)	0
Barbara	(48, 48)	0
Sailboat	(128, 128)	0.003
Parrots	(80, 80)	0.002
Fruits	(112, 112)	0.001
Parrot2	(40, 40)	0
Flower	(160, 160)	0.005
Natural	(160, 160)	0.003
Pepper3	(72, 72)	0
Colors	(80, 80)	0

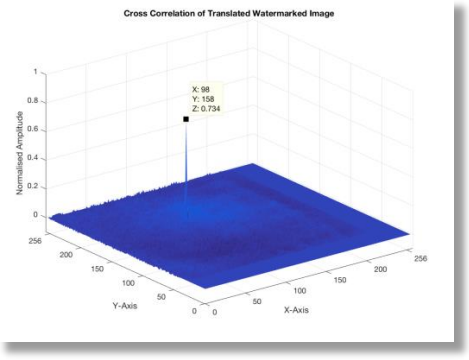
Figure 62 shows some examples of smaller images of size 256x256 that have been subjected to translation attacks.

Figure 62 Watermarked images of size 256x256 subjected to translation attacks: Lena (+40, -40), Pepper2 (+32, -32), Foods (+60, -60).

Figure 63 shows the cross-correlation results for the translated ‘Lena’, ‘Pepper2’ and ‘Foods’ images.



(a) **(b)**



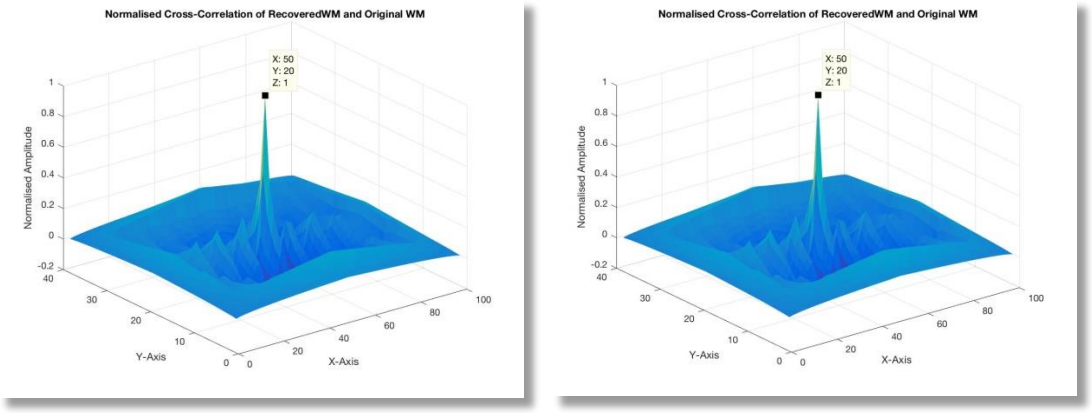
(c)

Figure 63 Detection of translation parameters through cross-correlation: (a) Lena (+40, -40), (b) Pepper2 (+32, -32), (c) Foods (+60, -60). The exact translation attack parameters are found by subtracting the height and width of the WTMM image from the values ‘X’ and ‘Y’ respectively.

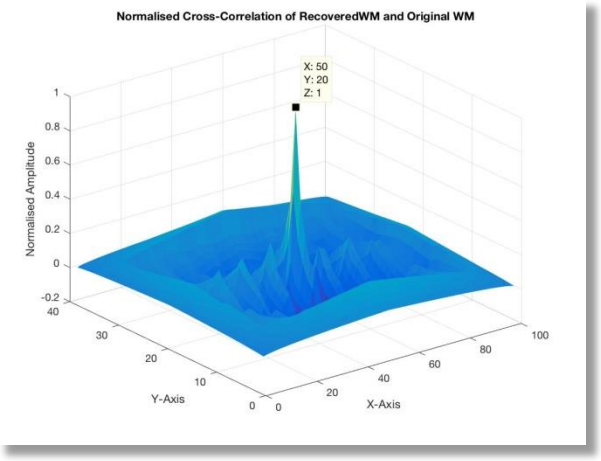
Figure 64 shows the restored watermarked images after undoing the translation attack. The information provided by the location of the cross-correlation peaks has been used to undo the attacks.

Figure 64 Restored watermarked images of size 256x256 after undoing the translation attacks: Lena (-40, +40), Pepper2 (-32 +32), Foods (-60, +60).

Figure 65 shows the normalized cross-correlation value of the recovered logo watermark after the translation attack has been undone. An NCC value of '1' is obtained in all three cases. The bit error rates corresponding to the NCC values in Figure 65 are shown in Table 11.



(a) **(b)**



(c)

Figure 65 Normalized Cross-Correlation (NCC) results between the recovered and the original logos after recovering the logo from a translation attack: (a) Lena (-40, +40), (b) Pepper2 (-32, +32), (c) Foods (-60, +60).

Table 11 Bit error rates corresponding to the NCC values in Figure 65**.**

Image	Distortion (Translation offset x, y)	Bit Error Rate (BER)
Lena	(40, 40)	0
Pepper2	(32, 32)	0
Foods	(60, 60)	0

The results in Figure 57 – Figure 65 demonstrate that the proposed watermarking scheme can successfully detect a watermark even if the cover image undergoes a translation attack.

6.6.3 Results for Different Wavelet and Multiwavelet Filters

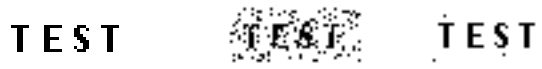
Different types of wavelets (orthogonal Daubechies (d4), Antonini 7.9 biorthogonal scalar wavelet filters) and multiwavelets (Cardbal2 balanced, Geronimo-Hardin-Massopust (GHM), Leburn-Vetterli balanced multiwavelet (BAT02)) were investigated for use in the proposed watermarking scheme.

Amongst the multiwavelets, the Cardbal2 multiwavelet offers the best results when taking into account attacks (See Table 12). As shown in Table 12, the Cardbal2 balanced multiwavelet was found to be slightly better than other multiwavelets such as Geronimo-Hardin-Massopust (GHM) and Leburn-Vetterli balanced multiwavelet (BAT02). Table 12 shows that Cardbal2 multiwavelet achieves an NCC value of 1 in most of the cases. On the other hand, for the GHM multiwavelet, the lowest NCC value is 0.51 (Sailboat, 0.4) while the overall range of NCC values is 0.8 – 1. For BAT02 multiwavelet, the lowest NCC is 0.38 (Sailboat, 0.4) while the overall range of NCC values is 0.9 – 1. So, from these results, it can be said that Cardbal2 multiwavelet achieves more stable NCC values for most of the type of attacks. Hence, among multiwavets, Cardbal2 was found to be the most suitable type for use in the proposed method.

Table 12 Performance comparison of different multiwavelet types (Cardbal2, GHM, and BAT02). Results are shown for 512x512 resolution images and the 'TEST' logo watermark.

Multi-Wavelet		Cardbal2					GHM					BAT02				
Attack / Image		**Lena**	**Pepper**	**Barbara**	**Airplane**	**Sailboat**	**Lena**	**Pepper**	**Barbara**	**Airplane**	**Sailboat**	**Lena**	**Pepper**	**Barbara**	**Airplane**	**Sailboat**
Rotation (Degree)	0.5º	1	1	1	1	1	1	1	1	1	1	1	1	1	0.99	0.98
	10.5º	1	1	1	1	0.98	1	0.99	0.99	1	0.97	0.99	0.99	1	1	0.98
	40º	0.98	1	0.99	0.95	0.97	0.98	0.98	0.99	0.97	0.95	0.99	0.98	0.98	0.95	0.95
	90º	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0.98
	115º	1	1	1	1	0.98	1	0.99	0.99	1	0.97	0.98	0.99	1	0.98	0.96
	120º	0.98	1	1	0.99	0.98	1	0.98	0.99	0.98	0.97	0.98	1	0.99	0.98	0.97
	160º	1	1	1	1	0.99	1	1	0.99	1	0.98	0.99	1	1	0.99	0.98
	250º	1	1	1	1	0.99	1	0.99	0.99	1	0.98	0.99	1	1	0.99	0.99
	300º	1	1	1	0.99	0.98	1	0.98	0.99	0.98	0.97	0.98	1	0.99	0.98	0.97
Scaling Factor	0.4	0.66	0.75	0.66	0.67	0.55	0.67	0.69	0.66	0.6	0.51	0.45	0.45	0.47	0.53	0.38
	0.5	1	1	0.97	1	0.95	0.94	0.93	0.88	0.91	0.74	0.97	0.98	0.98	0.92	0.89
	0.6	1	1	0.97	0.98	0.96	1	0.99	0.97	0.98	0.95	0.97	0.97	1	0.96	0.91
	0.75	1	1	0.98	1	0.98	1	1	0.99	1	0.97	0.99	0.98	1	0.99	0.95
	1.25	1	1	1	1	1	0.98	0.98	0.97	0.98	0.97	0.99	1	0.96	0.98	0.97
	1.4	0.99	0.98	0.94	0.99	0.94	0.99	0.98	0.96	0.99	0.94	0.98	0.98	0.94	0.95	0.94
	1.5	0.98	0.99	0.97	0.97	0.93	0.99	1	0.96	0.96	0.95	0.97	0.99	0.95	0.96	0.93
Translating (x, y)	(48, 48)	1	1	1	0.99	1	1	1	0.99	1	0.97	1	1	1	1	0.98
	(96, 96)	1	1	1	0.99	0.97	0.99	0.99	1	1	0.95	1	1	0.99	0.99	0.96
	(128, 128)	0.99	1	0.98	0.99	0.98	0.99	0.99	0.98	1	0.94	0.99	0.99	0.99	0.98	0.97
	(176, 176)	1	0.99	0.94	1	0.94	1	0.96	0.91	0.99	0.94	0.99	0.96	0.93	1	0.93

Next, the different types of wavelets were tested. The results obtained using the different wavelets are shown in Table 13 - Table 14. The experimental results were obtained by using the 'TEST' logo watermark for images of size 512x512. Table 13 presents the NCC values for rotation, scaling, and translation attacks using the 'Antonini 7.9' scalar wavelet for the 'TEST' logo watermark. From these results, it can be seen that for all the tested rotation angles, the NCC values are in the range of 0.8 – 0.9. In case of scaling attacks, the NCC values obtained are in the range of 0.81 - 0.98, except for the scaling factor of 0.2 for which the lowest NCC value is 0.55. In case of translation attacks, it can be seen from the results that the NCC values are in the range of 0.8 – 0.97. The recovered 'TEST' logo watermarks for different attacks are shown in Figure 66.



(a) **(b)** **(c)**

Figure 66 The recovered 'TEST' logo watermarks for the Antonini 7.9 wavelet: (a) The original logo watermark (b) Airplane (Scaling: 0.2; NCC: 0.55), (c) Barbara (Rotated: 150^{o}; NCC: 0.98).

Table 14 presents the results obtained for the 'Daubechies (d4)' scalar wavelet. The results are shown for different geometrical attacks (rotation, scaling, and translation) using the Daubechies (d4) scalar wavelet filter bank and the 'TEST' logo watermark. In case of rotation attacks, it can be seen that the NCC values obtained are in the range of 0.77 – 0.98. In case of scaling attacks, the NCC values are, again, in the range of 0.8 – 0.9. Lastly, in the case of translation attacks, the NCC values are in the range of 0.75 – 0.96. The recovered 'TEST' logo watermarks for different attacks are shown in Figure 67.

(a) **(b)** **(c)**

Figure 67 The recovered 'TEST' logo watermarks for the Daubechies (d4) wavelet: (a) The original logo watermark (b) Pepper (Scaling: 0.2; NCC: 0.43), (c) Barbara (Rotated: 15^{o}; NCC: 0.0.97).

Table 13 Normalized cross correlation (NCC) values for the recovered logo watermark after undergoing different amounts of rotation, scaling, and translation. The results are shown for 512x512 resolution images using the 'TEST' logo and the Antonini 7.9 scalar wavelet.

Attack \ Image		Lena	Pepper	Barbara	Airplane
Rotation (Degrees)	15^o	0.97	0.98	0.97	0.90
	35^o	0.88	0.91	0.94	0.77
	90^o	0.98	0.97	0.98	0.92
	150^o	0.93	0.96	0.98	0.82
	260^o	0.97	0.99	0.98	0.91
	340^o	0.97	0.97	0.98	0.89
Scaling Factor	0.2	0.65	0.66	0.66	0.55
	0.3	0.95	0.96	0.96	0.89
	0.5	0.97	0.97	0.98	0.92
	0.8	0.98	0.97	0.98	0.92
	1.2	0.94	0.96	0.95	0.81
Translation (x, y)	(80, 80)	0.95	0.97	0.95	0.86
	(112, 112)	0.92	0.95	0.92	0.85
	(160, 160)	0.88	0.89	0.88	0.80

Table 14 Normalized cross correlation (NCC) values for the recovered logo watermark after undergoing different amounts of rotation, scaling, and translation. The results are shown for 512x512 resolution images using the 'TEST' logo and the Daubechies (d4) wavelet.

Attack \ Image		Lena	Pepper	Barbara	Airplane
Rotation (Degrees)	15^o	0.96	0.97	0.97	0.91
	35^o	0.88	0.91	0.94	0.77
	90^o	0.98	0.98	0.98	0.94
	150^o	0.9	0.92	0.94	0.77
	260^o	0.96	0.98	0.97	0.91
	340^o	0.93	0.94	0.95	0.86
Scaling Factor	0.2	0.46	0.43	0.47	0.44
	0.3	0.88	0.86	0.87	0.77
	0.5	0.97	0.96	0.97	0.92
	0.8	0.98	0.98	0.96	0.94
	1.2	0.92	0.94	0.9	0.77
Translation (x, y)	(80, 80)	0.89	0.96	0.95	0.78
	(112, 112)	0.92	0.94	0.90	0.75
	(144, 144)	0.85	0.86	0.87	0.75

Finally, the results obtained using the Cardbal2 multiwavelet filter bank, are compared against the Antonini 7.9, and Daubechies (d4) scalar wavelet filter banks. In each case, the watermarked images are subjected to geometrical attacks (rotation, scaling, and translation). These results are presented in Figure 68 – Figure 70. In these tests, the following 512x512 size images are used: 'Lena', 'Pepper', 'Barbara', and 'Airplane'. The results shown in Figure 68 – Figure 70 are average results for these images. Moreover, the 'TEST' logo watermark is used. A variety of attack parameters are considered in these results i.e., both low and high strength geometrical attack parameters are used. The results clearly show that the Cardbal2 multiwavelet filter bank is the best choice for use in the proposed watermarking scheme as it outperforms the other types of wavelet filters tested.

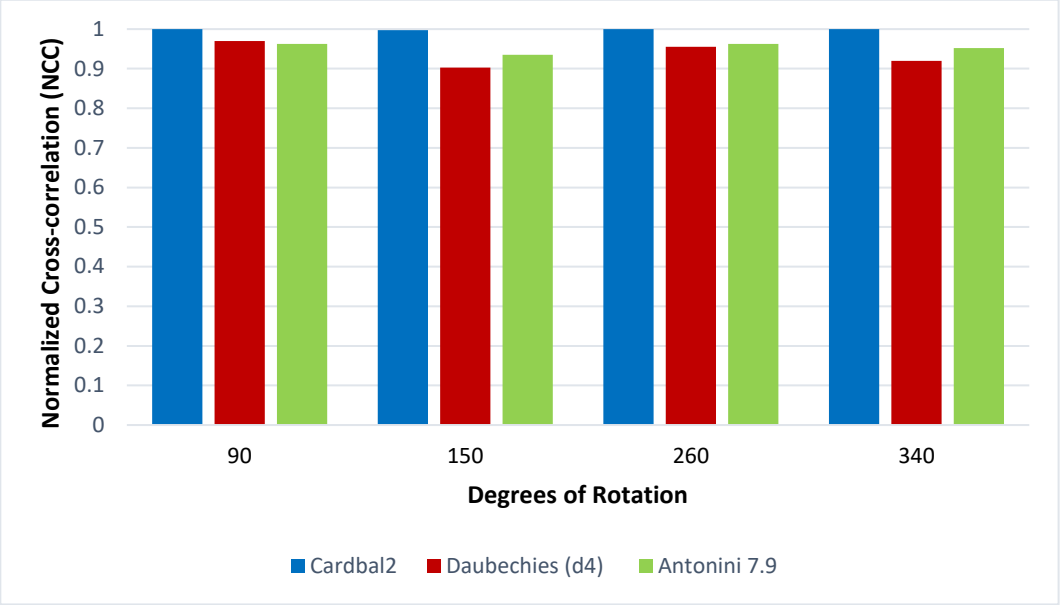


Figure 68 Comparison of the results obtained using different types of wavelet/multiwavelet filters. The results are obtained using the 'TEST' logo watermark and represent the averages figure of the four images used for this comparison.

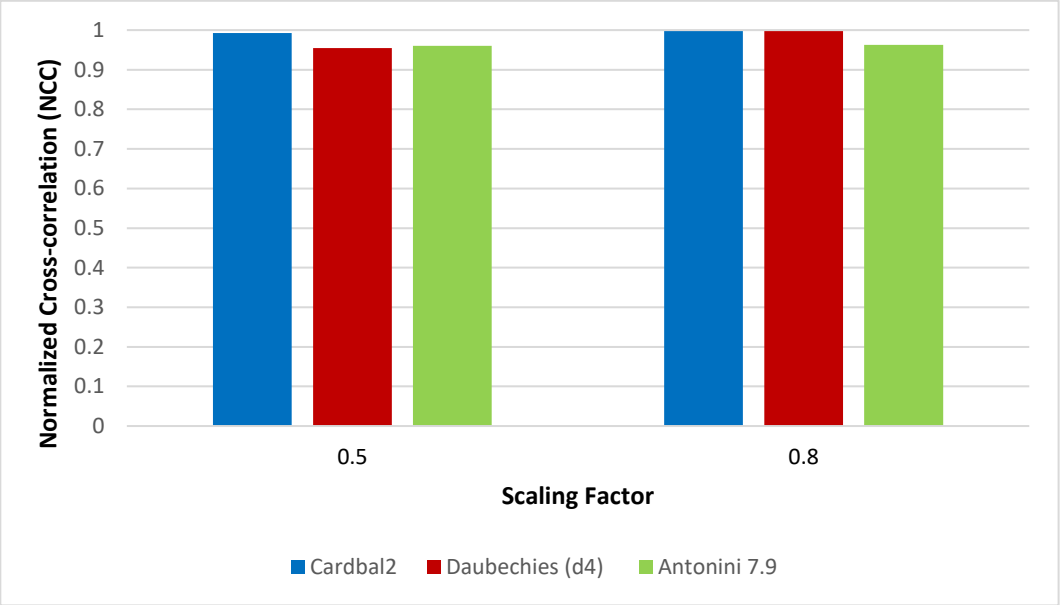


Figure 69 Comparison of the results obtained using different types of wavelet/multiwavelet filters. The results are obtained using the 'TEST' logo watermark and represent the averages figure of the four images used for this comparison.

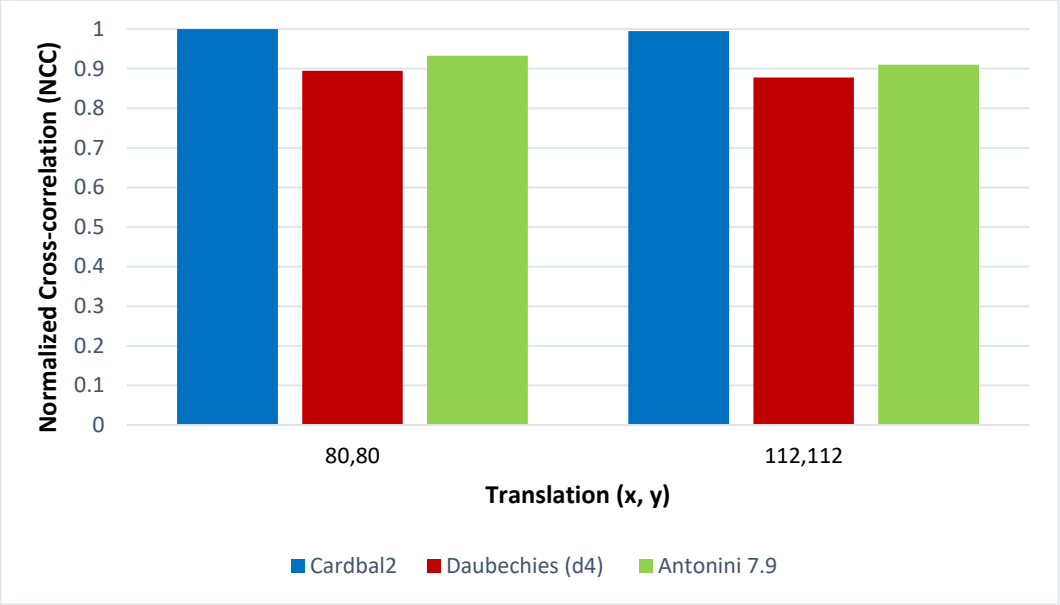


Figure 70 Comparison of the results obtained using different types of wavelet/multiwavelet filters. The results are obtained using the 'TEST' logo watermark and represent the averages figure of the four images used for this comparison.

As it can be clearly seen that Cardbal2 performs the best amongst all the tested wavelets and multiwavelets, hence, it is used in the proposed method. The results for the proposed method presented in the remaining chapter are obtained using Cardbal2 multiwavelet.

6.6.4 Comparison with Other Methods

In this section, the results of the proposed method are compared against other existing logo watermarking schemes, such as those presented in [55] and [77]. In [55] authors used 512x512 sized grayscale images 'Lena' and 'Pepper' with a 32x32 size watermark logo. The method described in [77] used 512x512 colour images with a 64x64 size binary watermark image. The results of the proposed method are first compared with those of [55]. This is followed by a comparison of the distortion parameter performance of the proposed method and the method outlined in [77].

The comparison results of the proposed method and the method in [55] are presented in Figure 71 – Figure 76. In these comparisons, the watermarked image 'Lena' is rotated at different angles and then the watermark is recovered from it. It is found that for the

proposed method, the lowest NCC value of 0.98 is obtained when the watermarked image is rotated by 50 degrees while in most of the other cases, an NCC value of 1 is achieved.

On the other hand, for [55], the lowest NCC value of 0.43 is obtained when the watermarked image is rotated by 110^{o} degrees while the highest NCC value is 0.53 when the watermarked image is rotated by 2^{o} degrees. As it can be seen from Figure 71, the proposed method outperforms [55] by a substantial margin for all rotation angles tested. Similar comparisons are presented for the 'Pepper' image in Figure 72. As it can be seen from these results, the proposed method significantly outperforms [55] again.

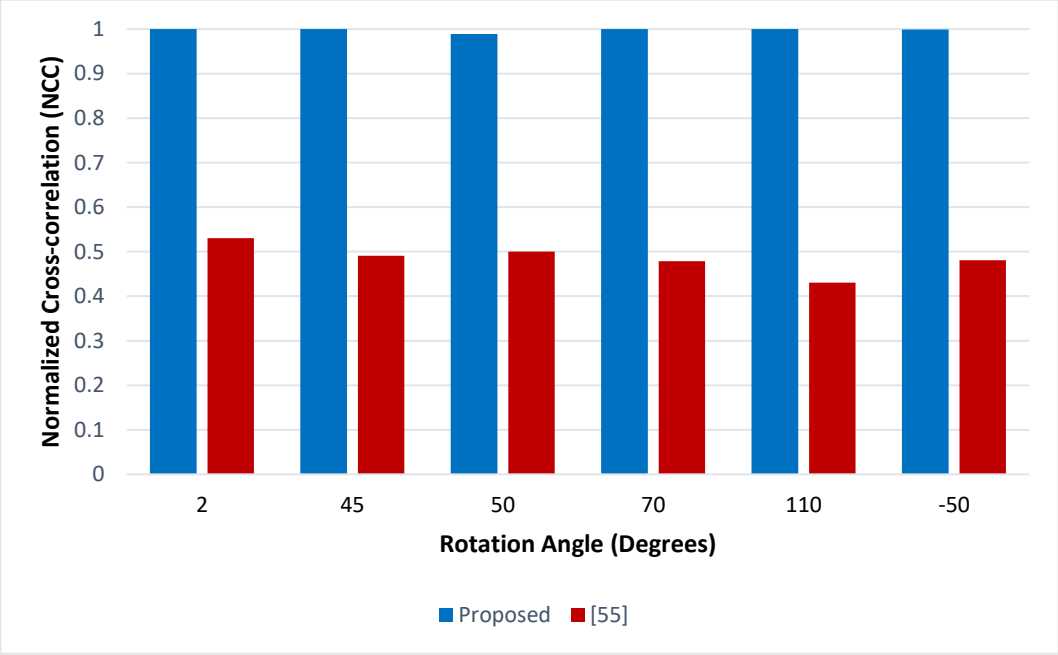


Figure 71 Robustness against rotation attacks of the proposed method compared to [55], for the 'Lena' image.

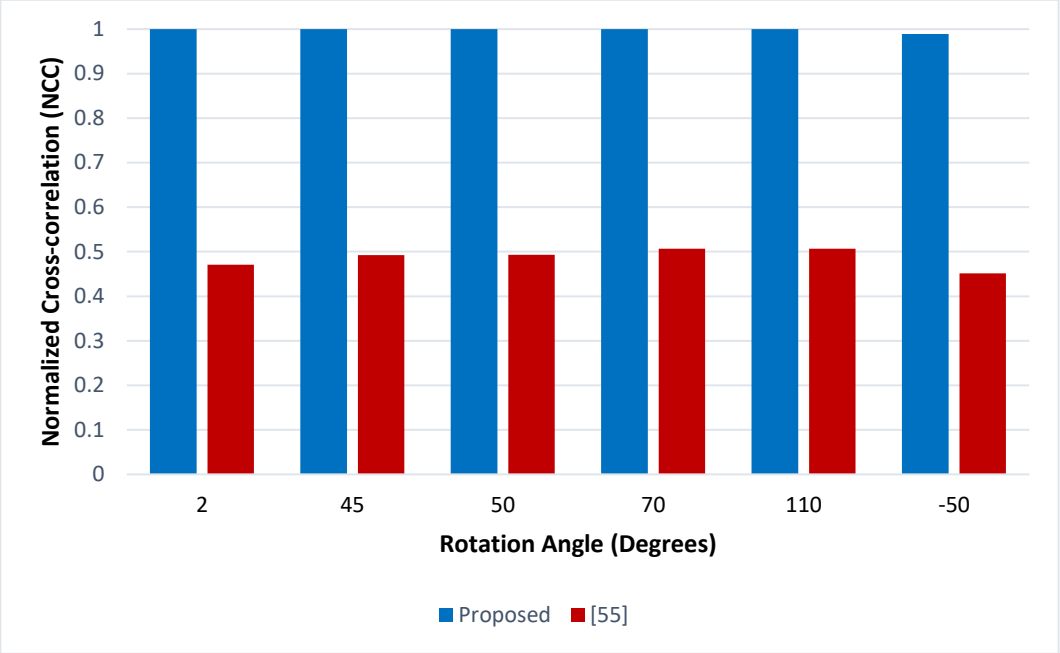


Figure 72 Robustness against rotation attacks of the proposed method compared to [55], for the 'Pepper' image.

Figure 73 – Figure 74 present the comparison results for scaling attacks. As it can be seen from the results presented in Figure 73, when the watermarked image 'Lena' is scaled by a factor of 0.5, both the proposed method and [55] achieve an NCC value of 1. The results for the watermarked image 'Pepper' are shown in Figure 74 for the same scaling factors as before. The proposed method achieves an NCC value of 1 while the method in [55] achieves an NCC value of 0.97. Hence, overall, the proposed method performs better.

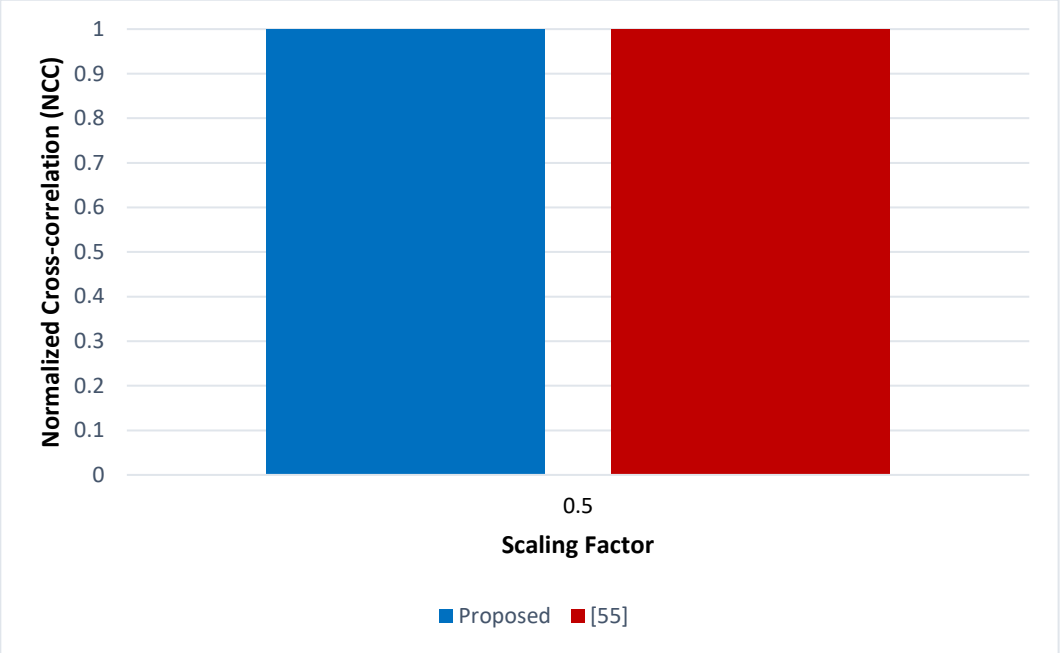


Figure 73 Robustness against scaling attacks of the proposed method compared to [55], for the 'Lena' image.

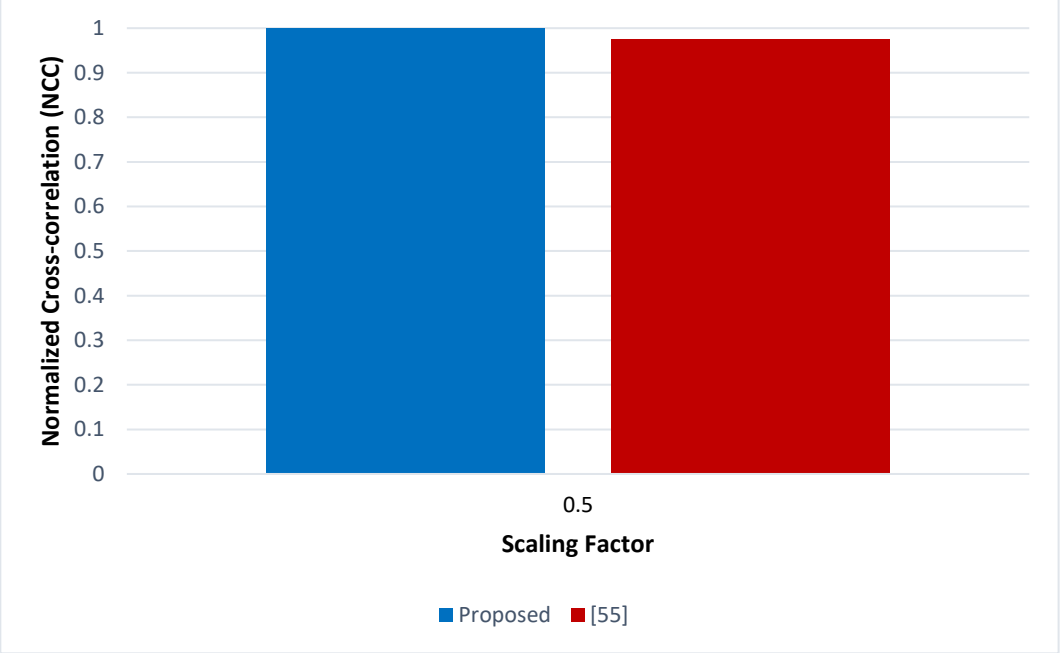


Figure 74 Robustness against scaling attacks of the proposed method compared to [55], for the 'Pepper' image.

Finally, Figure 75 and Figure 76 show the comparison results for translation attacks. Figure 75 shows the results for the 'Lena' image. It can be seen that the proposed technique achieves an NCC value of 1 for all of the attacks that were tested, while the method in [55] achieves considerably lower NCC values. A similar trend can be observed for the 'Pepper' image. Hence, overall, the proposed method significantly outperforms the method presented in [55].

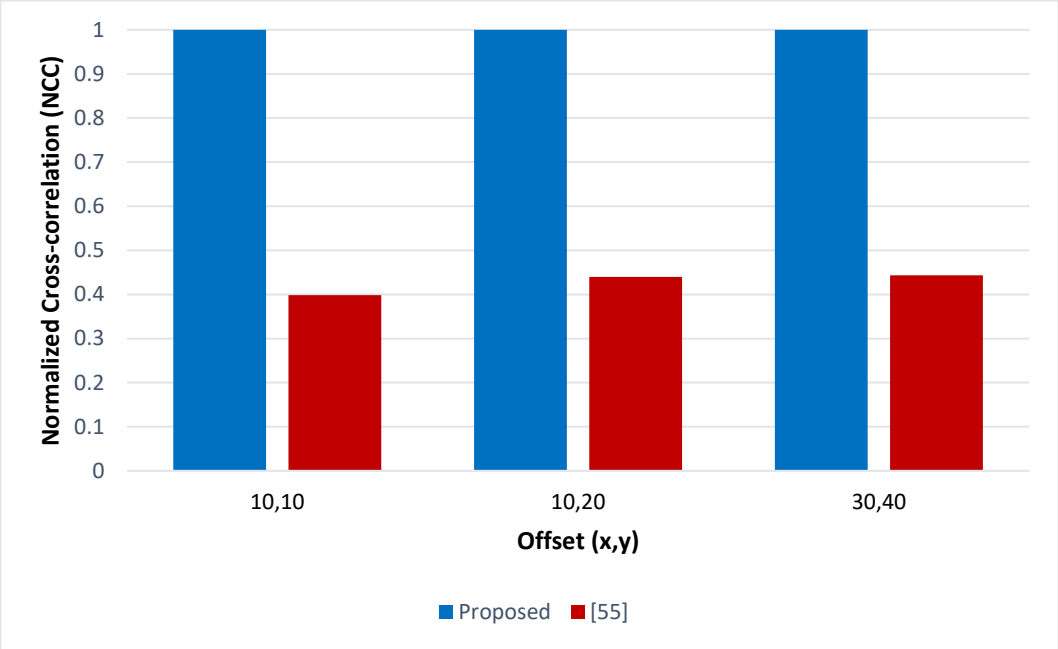


Figure 75 Robustness translation scaling attacks of the proposed method compared to [55], for the 'Lena' image.

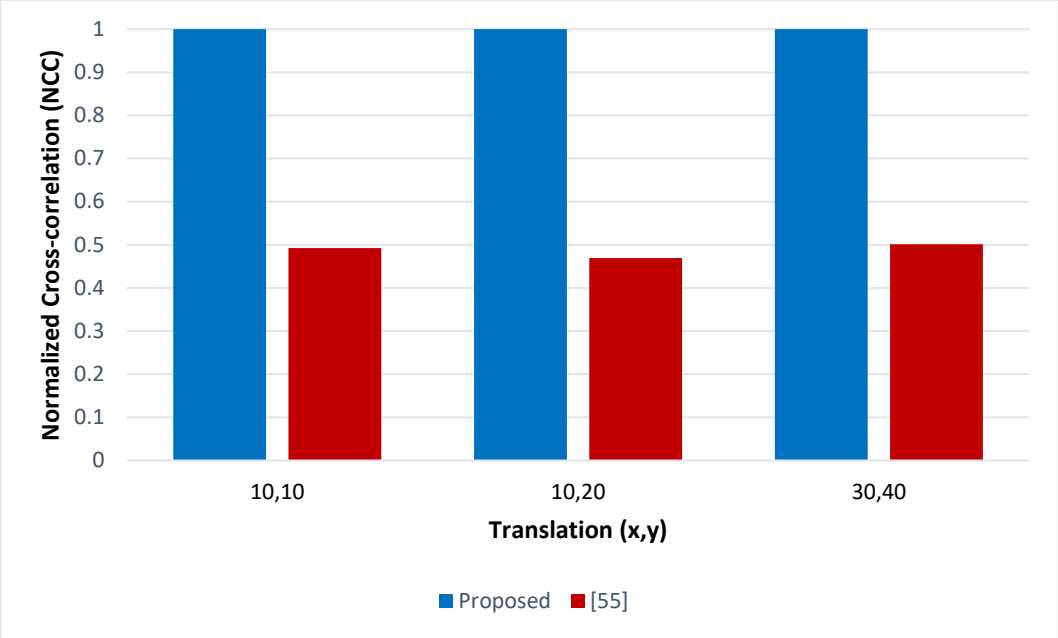


Figure 76 Robustness against translation attacks of the proposed method compared to [55], for the 'Pepper' image.

Figure 77 – Figure 79 present the distortion parameter detection performance comparison of the proposed method and the method presented in [77]. From the results in Figure 77 – Figure 79, it can be concluded that both methods perform almost equally well in detecting the degrees of rotation, the translation offsets, and the scaling factors.

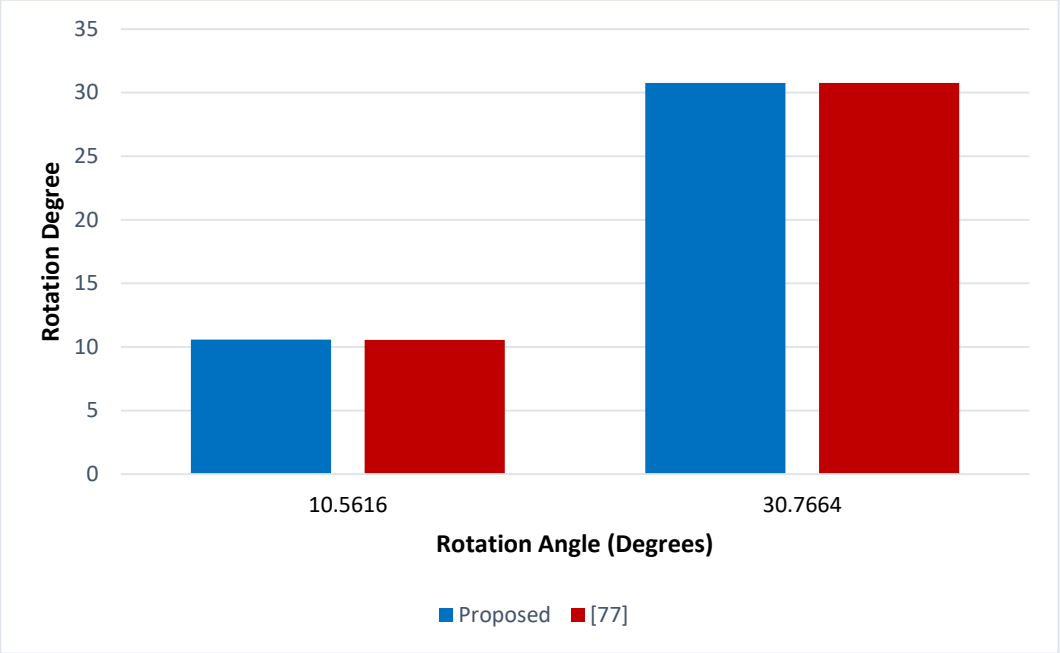


Figure 77 Robustness against rotation attacks of the proposed method compared to [77], for the 'Lena' image.

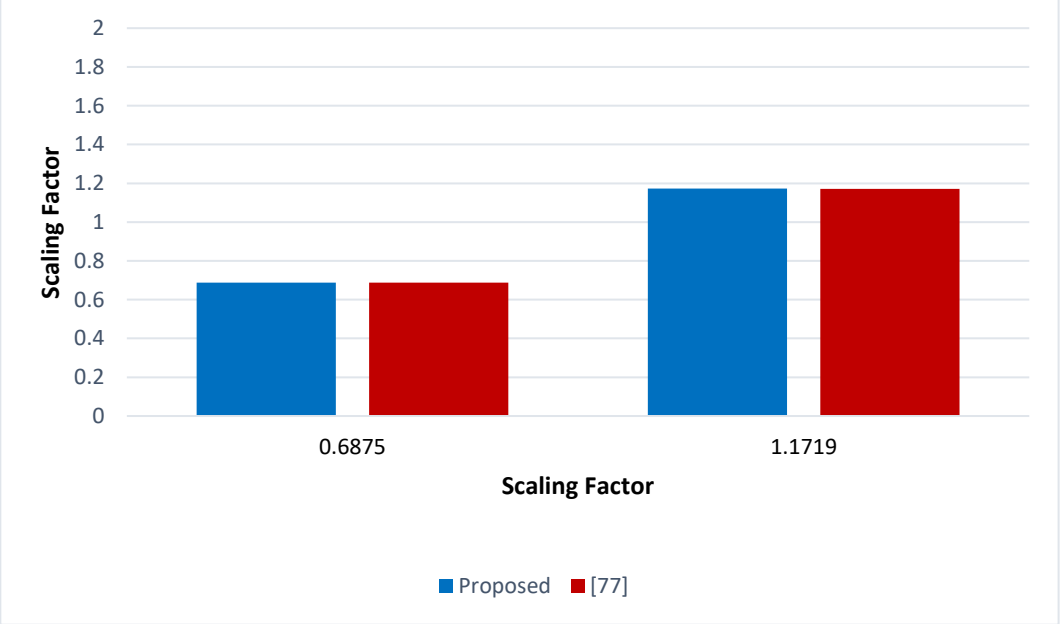


Figure 78 Robustness against scaling attacks of the proposed method compared to [77], for the 'Lena' image.

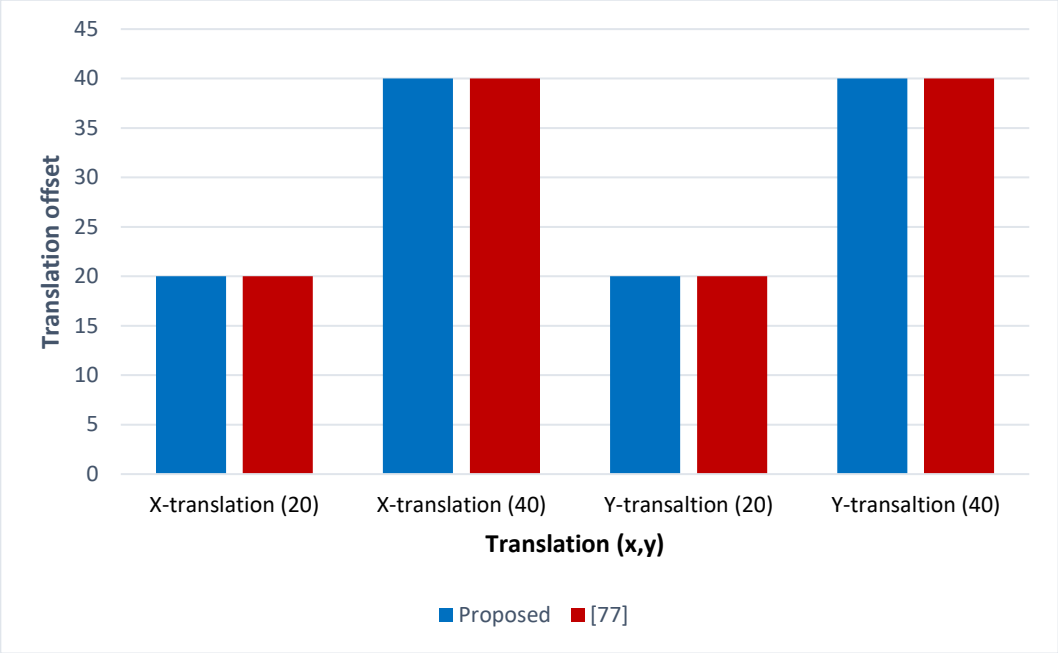


Figure 79 Robustness against translation attacks of the proposed method compared to [77], for the 'Lena' image.

Table 15 compares the robustness of the proposed method and the method from [77] in terms of the bit error rate (BER). The results are shown for the 'Lena' image. The results show that except for translation by (2, 15) and (15, 2), in all other cases, the proposed method outperforms the method in [77].

Table 15 Comparison of Bit Error Rates (BER) for the proposed method and the method in [77] for the Lena image.

Distortion		Proposed Bit Error Rate (BER)	[77] Bit Error Rate (BER)
Rotation (Degrees)	10º	0	0.0066
	15º	0	0.0066
	45º	0	0.0071
	70º	0	0.0059
	90º	0	0.0029
Scaling Factors	0.5	0	0.437
	0.9	0	0.0229
	1.2	0	0.0134
	1.4	0.002	0.0063
	1.5	0.003	0.0081
Translation (x, y)	(2, 15)	0.113	0.0029
	(15, 2)	0.116	0.0029
	(20, 20)	0	0.0029
	(50, 0)	0	0.0029
	(0, 50)	0	0.0029

The results of the proposed watermarking scheme are also compared with another state-of-the-art method [103]. These results are shown in Table 16. From these results, it can be seen that the proposed scheme generally performs better than the method in [103], especially when dealing with rotation attacks. For example, in Table 16, it can be seen that in case of rotation, the proposed method always outperforms the method in [103] except for the single case of the Lena image rotated by 30^{o} where the performance of the method in [103] is only marginally better than that of the proposed method. In terms of scaling, it can be seen that the proposed method performs better, especially for mid-range scaling factors. Finally, in the case of translation, the proposed method performs better in case of Lena image while the method in [103] performs slightly better in case of Barbara image. Hence, it can be said that, overall, the proposed method outperforms the method in [103].

Table 16 Comparison of Normalized Cross-Correlation (NCC) values for the proposed method and the method in [103] for the Lena and Barbara images.

Distortion		Lena		Barbara	
		Proposed Normalized Cross-Correlation (NCC)	**[103]** Normalized Cross-Correlation (NCC)	**Proposed** Normalized Cross-Correlation (NCC)	**[103]** Normalized Cross-Correlation (NCC)
Rotation (Degrees)	2º	1	0.9741	1	0.9703
	5º	1	0.9813	1	0.9659
	10º	1	0.9861	0.99	0.9738
	30º	0.98	0.9861	1	0.9822
	45º	1	0.9828	0.99	0.9822
Scaling Factors	0.25	0.153	0.437	0.21	0.9713
	0.5	1	0.9744	0.97	0.991
	0.9	1	0.9919	1	0.9731
	1.2	1	0.9931	0.98	0.9726
Translation (x, y)	(0, 128)	1	0.9954	0.98	0.9962
	(128, 0)	1	0.9964	0.98	0.9962

Finally, the proposed watermarking scheme is also compared with the state-of-the-art method described in [90]. The comparison results are shown in Table 17. From the results in Table 17, it can be concluded that in case of rotation and translation attacks, the proposed method always outperforms the method in [90] while in case of translation attacks, the proposed method may or may not outperform the method in [90] depending on the situation.

Table 17 Comparison of Bit Error Rate (BER) values for the proposed method and the method in [90] for the Lena and Barbara images.

Distortion		Lena		Barbara	
		Proposed Bit Error Rate (BER)	**[90]** Bit Error Rate (BER)	**Proposed** Bit Error Rate (BER)	**[90]** Bit Error Rate (BER)
Rotation (Degrees)	10º	0	0.0144	0.001	0.0264
	15º	0	0.0159	0	0.0342
	45º	0	0.0293	0.001	0.0823
	70º	0	0.0164	0	0.0378
	90º	0	0.0068	0	0.0049
Scaling Factors	0.5	0	0.0671	0.005	0.1023
	0.9	0	0.0474	0	0.0369
	1.2	0	0.0369	0.002	0.0374
	1.4	0.001	0.0378	0.01	0.0381
	1.5	0.003	0.041	0.004	0.0417
Translation (x, y)	(2, 15)	0.113	0.0068	0.13	0.0056
	(15, 2)	0.116	0.0068	0.132	0.0051
	(20, 20)	0	0.0088	0	0.0103
	(50, 0)	0	0.0073	0	0.009
	(0, 50)	0	0.0068	0	0.0093

6.6.5 Overall Results

The overall results of the proposed algorithm are shown in Table 18 – Table 21. The results are shown for both the ‘TEST’ and ‘ME’ logo watermarks as well as for both 512x512 and 256x256 resolution cover images. The logo is embedded using the Cardbal2 multiwavelet. This choice was made after conducting tests with other types of wavelets (including Daubechies (d4) and Antonini 7.9 scalar wavelets) and multiwavelets (including GHM and BAT02). As shown in Table 12 and Figure 68 – Figure 70 in Section 6.6.3, the Cardbal2 multiwavelet filter produced much better results compared to the Daubechies (d4) and Antonini 7.9 scalar wavelets and better results compared to other multiwavelets.

Table 18 presents the normalized cross correlation (NCC) values obtained after recovering the logo image after undergoing different types of attacks. These results are shown for 512x512 resolution images and the 'TEST' logo watermark using the Cardbal2 multiwavelet filter bank. It can be seen from the results in Table 18 that the logo watermark can be efficiently recovered using the proposed watermarking scheme. For example, in the case of rotation, the cover image was rotated by different degrees and the embedded logo image was recovered in each case with a high normalized cross-correlation (NCC) value. For many of the tested cover images and for most degrees of rotation, the watermark was successfully recovered with an NCC value of 1. In all the cases of rotation, the watermark was recovered with an NCC value of at least 0.9.

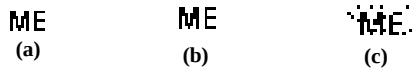
In the case of scaling, the cover images were scaled by a factor in the range of 0.4 to 1.9. For each scaling factor, the watermark was successfully recovered with a high NCC value. The maximum NCC value of 1 was obtained in most cases while lower NCC values were observed for smaller scaling factors (i.e. scaling factors lower than 1). In the case of translation, the cover images were translated by different amounts as shown in Table 13. The logo watermark image was recovered successfully in each case. For most of the translation offset values and for most of the images, the watermark was recovered with an NCC value of 1 while in all remaining cases, the watermark was still recovered with a NCC value in excess of 0.9. These results show that the proposed method can recover high fidelity watermarks with an NCC value of at least 0.9 even after undergoing severe RST attacks. The recovered 'TEST' logo watermarks for different cases are shown in Figure 80**.**

(a) **(b)** **(c)** **(d)** **(e)**

Figure 80 The recovered 'TEST' logo watermarks: (a) The original logo watermark (b) Lena (Rotation: 40^{o}; NCC: 0.98), (c) Barbara (Translation: 144, 144; NCC: 0.97) (d) Lena (Scaling: 0.4; NCC: 0.66), (e) Pepper3 (Scaling: 0.4; NCC: 0.75).

Even better results were obtained when watermarking 512x512 size cover images with the smaller 'ME' logo image (see Table 19), when due to the much smaller logo the embedding chip rate is substantially higher. As it can be seen from Table 19, for most of

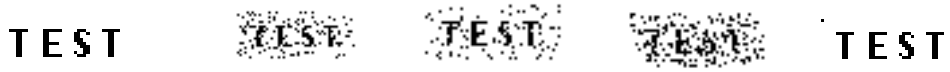
the geometrical attacks an NCC value of 1 is obtained. For rotation attacks, the lowest NCC value is 0.98, while for most test cases of rotation an NCC value of 1 is achieved. For scaling attacks, equally encouraging results were obtained. High NCC values were now obtained even for more severe amounts of scaling. In case of translation attacks, the lowest NCC was 0.97. The recovered 'ME' logo watermarks for different cases are shown in Figure 81.



(a) (b) (c)

Figure 81 The recovered 'ME' logo watermarks: (a) The original logo watermark (b) Sailboat (Rotation: 140^{o}; NCC: 0.98), (c) Sailboat (Scaling: 0.4; NCC: 0.81).

The results for 256x256 resolution images are shown in Table 20 for the 'TEST' logo watermark and in Table 21 for the 'ME' logo watermark. From Table 20, it can be seen that in case of rotation attacks, the lowest NCC value was 0.91, while for most of the other cases NCC values of 1 are obtained. In the case of scaling attacks, it can be noticed from the results that when the image is scaled up (scaling factors >1), the NCC value of 1 is obtained, but predictably, when the images are scaled down, the NCC value decreases. For example, at a scaling factor of 0.7, NCC values of 0.64, 0.73, and 0.55 are observed. The recovered 'TEST' logo watermarks for different cases are shown in Figure 82.



(a) (b) (c) (d) (e)

Figure 82 The recovered 'TEST' logo watermarks in case of 256x256 size cover images: (a) The original logo watermark (b) Lena (Scaling: 0.7; NCC: 0.56), (c) Pepper2 (Scaling: 0.7; NCC: 0.66), (d) Foods (Scaling: 0.7; NCC: 0.43) and (e) Foods (Rotation: 110^{o}; NCC: 0.99).

As the watermarked image is already small in size i.e., 256x256 and the 'TEST' logo watermark is used, the chip rate decreases and as we scale the image down further, this starts affecting the logo which for more aggressive scaling factors gets destroyed in the process. In the case of translation attacks, encouraging results are observed in most situations, as an NCC value of 1 is obtained in most cases.

Table 20 shows the results obtained using the 'ME' logo which is a much smaller watermark compared to the 'TEST' logo. In this case, the chip rate is much higher and it

can be noticed from the table that the NCC results have improved. For the case of rotation, an NCC of 1 is obtained for all rotation angles. In the case of scaling attacks, all scaling factors larger than 1 result in an NCC value of 1. As it can be seen from Table 20, when the watermarked image is scaled down to a smaller size with a scaling factor of 0.5, significantly smaller NCC values are achieved. This is because the size of the watermarked image is now reduced to half (i.e., 128x128) which is too small to reliably accommodate even the smaller 'ME' logo.

The recovered 'ME' logo watermarks for different cases of scaling are shown in Figure 83.

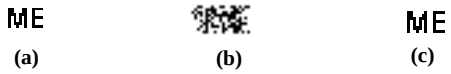


Figure 83 The recovered 'ME' logo watermarks for 256x256 resolution images: (a) The original logo watermark (b) Lena (Scaling: 0.5; NCC: 0.29), (c) Foods (Scaling: 0.8; NCC: 0.98).

For translation attacks, NCC value of 1 are obtained for all the translation attack result provided in the table.

Table 18 Normalized cross correlation (NCC) values for the recovered logo watermark after undergoing different amounts of rotation, scaling, and translation. The results are shown for 512x512 resolution images using the 'TEST' logo and the Cardbal2 balanced multiwavelet.

Attack \ Image		Lena	Pepper	Barbara	Airplane	Sailboat	Parrots	Parrot2	Natural	Fruits	Pepper3	Flower	Colors
Rotation (Degrees)	10^o	1	1	0.99	1	0.98	0.99	1	1	0.99	1	1	1
	20^o	1	1	0.99	1	0.99	0.99	1	1	1	1	1	1
	30^o	0.98	1	1	0.99	0.98	0.99	1	1	1	1	0.99	0.98
	40^o	0.98	1	0.98	0.95	0.97	0.98	0.98	0.97	0.98	0.98	0.98	0.95
	50^o	0.98	1	0.98	0.97	0.97	0.97	1	0.99	0.98	0.98	1	0.98
	60^o	1	1	0.99	1	0.99	0.99	1	1	0.98	1	1	0.99
	70^o	1	1	1	1	0.99	1	1	1	0.98	1	1	1
	80^o	1	1	1	1	1	0.99	1	1	0.98	1	1	1
	90^o	1	1	1	1	1	1	1	1	0.99	1	1	1
	100^o	1	1	0.99	1	0.98	0.99	1	1	0.99	1	1	1
	110^o	1	1	0.99	1	0.99	0.99	1	1	1	1	1	1
	120^o	0.98	1	1	0.99	0.98	0.99	1	1	1	1	0.99	0.98
	130^o	0.98	0.98	0.98	0.95	0.97	0.98	0.98	0.97	0.98	0.98	0.98	0.95
	140^o	0.98	1	0.98	0.97	0.97	0.97	0.99	0.99	0.98	0.98	1	0.98
	150^o	1	1	0.99	1	0.99	0.99	1	1	0.98	1	1	0.99
	160^o	1	1	1	1	0.99	1	1	1	0.98	1	1	1
	170^o	1	1	1	1	1	0.99	1	1	0.98	1	1	1
	180^o	1	1	1	1	1	1	1	1	0.99	1	1	1
	190^o	1	1	0.99	1	0.98	0.99	1	1	0.99	1	1	1
	200^o	1	1	0.99	1	0.99	0.99	1	1	1	1	1	1
	210^o	0.98	1	1	0.99	0.98	0.99	1	1	1	1	0.99	0.98
	220^o	0.98	0.98	0.98	0.95	0.97	0.98	0.98	0.97	0.98	0.98	0.98	0.95
	240^o	1	1	0.99	1	0.99	0.99	1	1	0.98	1	1	0.99

	260^o	1	1	1	1	1	0.99	1	1	0.98	1	1	1
	280^o	1	1	0.99	1	0.98	0.99	1	1	0.99	1	1	1
	300^o	1	1	1	0.99	0.98	0.99	1	1	1	1	0.99	0.98
	320^o	0.98	1	0.98	0.97	0.97	0.97	1	0.99	0.98	0.99	1	0.98
	340^o	1	1	1	1	0.99	1	1	1	0.98	1	1	1
	350^o	1	1	1	1	1	0.99	1	1	0.98	1	1	1
	355^o	1	1	1	1	1	1	1	1	0.98	1	1	1
Scaling Factor	0.4	0.66	0.75	0.66	0.67	0.55	0.69	0.88	0.65	0.57	0.75	0.69	0.65
	0.5	1	1	0.97	1	0.95	1	1	0.99	0.98	1	1	0.99
	0.6	1	1	0.97	0.98	0.96	0.97	1	1	0.96	1	0.99	1
	0.7	1	1	0.98	1	0.99	0.99	1	0.99	0.98	1	1	0.99
	0.8	1	1	0.99	1	0.98	1	1	1	1	1	1	1
	0.9	1	1	1	1	1	1	1	1	0.98	1	1	0.99
	1.1	1	1	0.99	1	0.98	0.99	1	1	0.98	1	1	1
	1.2	1	1	0.98	0.99	0.98	1	1	1	0.95	0.99	1	1
	1.3	1	1	0.97	1	0.97	0.97	1	1	0.95	0.99	1	0.99
	1.4	0.99	0.98	0.94	0.99	0.94	0.97	1	1	0.94	1	0.98	0.98
	1.5	0.98	0.99	0.97	0.97	0.93	0.96	1	0.98	0.91	1	0.98	0.97
	1.6	0.97	0.99	0.93	0.92	0.90	0.93	1	0.94	0.87	0.97	0.97	0.96
	1.7	0.97	0.99	0.95	0.97	0.90	0.91	1	0.95	0.85	0.98	0.97	0.95
	1.8	0.96	1	0.95	0.94	0.86	0.88	1	0.95	0.82	0.97	0.96	0.96
	1.9	0.97	0.98	0.94	0.95	0.83	0.84	1	0.94	0.77	0.98	0.94	0.93
Translation (x, y)	(32, 32)	1	1	1	1	1	0.99	1	1	0.98	1	1	1
	(64, 64)	1	1	1	0.99	1	0.98	1	1	0.97	1	1	1
	(80, 80)	1	1	1	1	0.99	0.98	1	0.99	0.98	1	1	1
	(112, 112)	1	1	0.99	0.99	0.97	0.97	1	0.98	0.99	1	0.99	0.98
	(128, 128)	0.99	1	0.98	0.99	0.98	0.98	1	0.98	0.98	1	0.99	0.98
	(144, 144)	0.99	1	0.97	0.99	0.97	0.98	1	0.98	0.97	1	0.98	0.97
	(176, 176)	0.99	0.99	0.94	1	0.94	0.98	1	0.97	0.97	1	0.95	0.95
	(208, 208)	0.97	0.97	0.92	0.99	0.90	0.96	1	0.95	0.96	0.98	0.93	0.94

Table 19 Normalized cross correlation (NCC) values for the recovered logo watermark after undergoing different amounts of rotation, scaling, and translation. The results are shown for 512x512 resolution images using the 'ME' logo and the Cardbal2 balanced multiwavelet.

Attack \ Image		Lena	Pepper	Barbara	Airplane	Sailboat	Parrots	Parrot2	Natural	Fruits
Rotation (Degrees)	10^o	1	1	1	1	1	1	1	1	1
	35^o	1	1	1	0.98	1	1	1	1	1
	45^o	1	1	1	1	1	1	1	1	1
	90^o	1	1	1	1	1	1	1	1	1
	140^o	1	1	1	1	0.98	1	1	1	1
	180^o	1	1	1	1	1	1	1	1	1
	225^o	1	1	1	1	1	1	1	1	1
	335^o	1	1	1	1	1	1	1	1	1
Scaling Factor	0.4	0.90	0.93	0.90	0.90	0.81	0.93	0.97	0.91	0.90
	0.5	1	1	1	1	1	1	1	1	1
	0.7	1	1	1	1	1	1	1	1	1
	1.5	1	1	1	1	0.98	1	1	1	1
	1.7	1	1	1	0.98	0.97	0.98	1	1	0.94
	1.9	1	1	1	1	0.95	0.95	1	1	0.90
Translation (x, y)	(64, 64)	1	1	1	1	1	1	1	1	1
	(120, 120)	1	1	1	1	1	1	1	1	1
	(208, 208)	1	1	0.98	1	0.98	1	0.97	1	1

Table 20 Normalized cross correlation (NCC) values for the recovered logo watermark after undergoing different amounts of rotation, scaling, and translation. The results are shown for 256x256 resolution images using the 'TEST' logo and the Cardbal2 balanced multiwavelet.

Attack \ Image		Lena	Pepper2	Foods
Rotation (Degrees)	10^o	1	1	0.99
	30^o	0.96	0.98	0.96
	50^o	0.93	0.97	0.92
	70^o	1	1	0.99
	90^o	1	1	1
	110^o	0.99	1	0.99
	140^o	0.93	0.97	0.92
	160^o	1	1	0.99
	180^o	1	1	1
	220^o	0.91	0.98	0.95
	240^o	0.99	1	0.97
	280^o	1	1	0.99
	310^o	0.91	0.98	0.95
	350^o	1	1	1
Scaling Factor	0.7	0.56	0.66	0.43
	1.1	1	1	1
	1.2	1	1	1
	1.3	1	1	0.99
	1.4	1	1	0.99
	1.6	0.99	1	1
Translation (x, y)	(40, 40)	1	1	1
	(80, 80)	1	1	1
	(104, 104)	1	1	0.99
	(120, 120)	1	1	0.99

Table 21 Normalized cross correlation (NCC) values for the recovered logo watermark after undergoing different amounts of rotation, scaling, and translation. The results are shown for 256x256 resolution images using the 'ME logo and the Cardbal2 balanced multiwavelet.

Attack \ Image		Lena	Pepper2	Foods
Rotation (Degrees)	10^o	1	1	1
	25^o	1	1	1
	45^o	1	1	1
	90^o	1	1	1
	130^o	1	1	1
	180^o	1	1	1
	250^o	1	1	1
	340^o	1	1	1
Scaling Factor	0.5	0.29	0.39	0.33
	0.8	0.98	1	0.98
	1.2	1	1	1
	1.6	1	1	1
	1.9	1	1	1
Translation (x, y)	(40, 40)	1	1	1
	(80, 80)	1	1	1
	(120, 120)	1	1	1

6.6.6 Time Complexity Analysis

In order to analyse the time-complexity of the proposed watermarking scheme, the average embedding and recovery times are investigated. These time values correspond to the average of several tests performed using a number of different host images and include both watermarks.

These results have been obtained by running the watermarking code on a MacBook Pro computer with a 2.2 GHz Intel Core i7 microprocessor, 16 GB DDR3 RAM, Intel Iris Pro 1536 MB graphics card and OS X El Capitan operating system, running MATLAB R2016.

The test results reveal that, on average, embedding of both watermarks in a host image takes around 90 seconds. In case of no attack, the embedded logo can be recovered on average in around 55 seconds. The total average time for both embedding and recovery (assuming no attack) is therefore 145 seconds (See Figure 84).

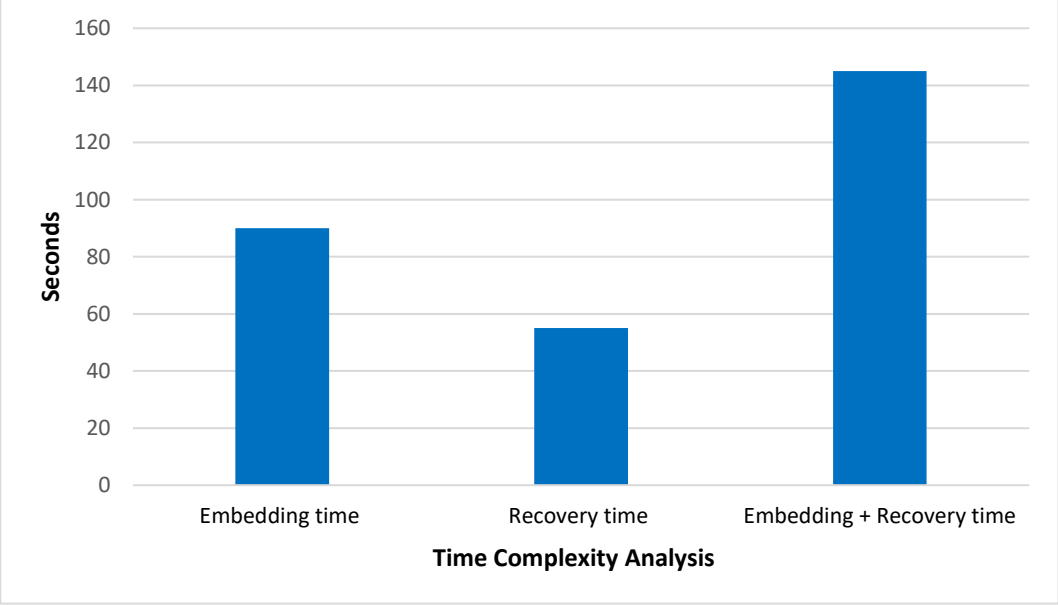


Figure 84 Average computational time of the proposed watermarking scheme

In case of a geometrical attack, the recovery time will very much depend on the search step size selected for each attack and the range of the attack parameters that are selected when carrying out this search.

The time-complexity of the proposed watermarking scheme is further illustrated with the aid of an example. In this example, the Lena image (with a resolution of 512×512) is subjected to a rotation attack and the proposed scheme is used to detect the rotation parameter and to correct it. It should be noted that in this example, a step size of 1 was used for detecting the rotation parameter while the total number of steps was 360. It takes the proposed scheme around 90 seconds in total to detect the rotation parameter and to correct the image. The same experiment is repeated again with a step size of 0.1 (corresponding to 3600 steps). and the detection and recovery time increases to 300 seconds. Hence, the time-complexity of the proposed scheme depends on the step size which is used. For example, decreasing the step size from 1 to 0.1 increased the number of steps 10 folds (from 360 to 3600) while the overall time increased 3.33 times (i.e., $\frac{300}{90} = 3.33$). Large step sizes result in lower computational complexities but they cannot be used for detecting small rotation angles. Similarly, small step sizes result in higher computational complexities but they can be used for detecting small rotation angles.

CHAPTER 7: CONCLUSIONS

This chapter presents an overview of the thesis and the conclusions of this research. A summary of all the chapters of the thesis is presented first. This is followed by the main conclusions drawn from this research. The last section discusses the limitations of the research presented in this thesis as well as suggestions for future work.

7.1 Summary of the Thesis

The thesis consists of seven chapters. A summary of the previous six chapters is presented in this section.

Chapter 1 introduced the topic of image watermarking and its applications. It also introduced the key research questions for this thesis which were mainly focused on proposing new approaches for robust logo image watermarking. The scope of the thesis, its main aims and objectives and the outline of this thesis were also presented in this chapter.

In Chapter 2, the fundamental concepts related to robust watermarking were presented. These included the main components of a basic watermarking scheme (such as watermark embedding and detection), classification of various watermarking schemes, and the most important properties of watermarking schemes, including, but not limited to perceptual transparency, blindness, robustness and capacity. Moreover, some of the main applications of watermarking techniques (such as protection of intellectual property rights, content verification, information hiding, and labelling) and the various types of attacks that they can be subjected to were also discussed in this chapter.

In Chapter 3, a literature review of state-of-the-art watermarking techniques was presented. Both spatial and transform domain methods were covered. It was concluded that transform domain techniques typically provided higher robustness compared to spatial domain techniques.

On the other hand, spatial domain techniques were found to be less complex and simpler to implement compared to transform domain techniques.

It was also concluded that Discrete Wavelet Transform (DWT) based methods for RGB coloured images can be improved further by considering the embedding of more than one watermark, by taking the Human Visual Systems (HVS) into consideration, and by using the shift-invariant property of Wavelet Transform Modulus Maxima (WTMM).

Chapter 4 introduced the basic concepts and mathematical background related to WTMM. This chapter also included a discussion about the practical considerations and the algorithmic implementation of the WTMM and presented a number of examples.

Chapter 5 presented in detail the proposed robust logo image watermarking scheme, covering both watermark embedding and detection and the novel technique employed to detect and undo geometrical attacks.

Chapter 6 presented and discussed the results obtained for the proposed watermarking scheme. Detailed results were presented which demonstrated the robustness of the proposed logo image watermarking scheme to geometrical attacks.

7.2 Main Conclusions

The main conclusions that can be drawn from this thesis are:

- By embedded a watermark in RGB colour images, the chip rate associated with a spread spectrum system can be increased three-fold compared to embedding the watermark in a grayscale image. This can improve the cross-correlation performance and the robustness of the watermark.

- The single-bit watermark can be used to detect whether an attack has taken place or not, while the multi-bit watermark can carry the actual logo watermark.

- HVS consideration should be included while designing a watermarking scheme. Especially, in the case of logo, since the watermark is inspected visually, it is no longer required that the recovered watermark be an exact copy of the embedded

watermark. Rather, a certain amount of loss, which is not visually significant, can be tolerated.

Due to the unequal sensitivity of the human eyes to changes in different colours, the proposed method used different weight factors for the red, green, and blue components. It was found that the green colour should be assigned the smallest weight while the blue colour should be assigned the highest weight. This weight assignment is also consistent with the fact that human eyes are more sensitive to changes in the green colour and least sensitive to changes in the blue colour.

- It has been demonstrated that embedding a 1-bit watermark in the WTMM coefficients can be successfully used to accurately detect and undo the attack parameters used by RST geometrical attacks on the watermarked images.

- Embedding a logo has the advantage of exploiting the error correction and pattern recognition capabilities of the HVS, which are used as a 'free' error correction code to build a certain degree of tolerance to error for the embedded logos.

7.3 Limitations and Suggestions for Future Work

This section presents the limitations of this study and also lays down suggestions for future work. One of the main limitations of the proposed logo image watermarking scheme is that it may not be able to efficiently recover watermark from a watermarked image when the image has been significantly scaled down. This is because the size of the watermarked image is might become too small to reliably accommodate the logo. When an image is scaled down, the chip rate decreases and at some point, scaling down further will start affecting the logo. Hence, for more aggressive scaling factors, the logo might get destroyed in the process of scaling down.

A possible solution for this would be to use more sub-bands for the embedding of the logo, including perhaps the approximation sub-band. The motivation for this idea is that having a copy of the watermark in multiple sub-bands could be useful in the case where the watermark embedded in one of the sub-bands is destroyed. In such a case, the watermark embedded in a different sub-band can be recovered. Furthermore, by having

more coefficients available to embed the watermark, the chip rate will increase and as a result the robustness of the watermark will increase. The idea of using more sub-bands for embedding is also in line with the spread spectrum philosophy, which relies on a large spread in order to better withstand any attacks. By embedding the watermark in more sub-bands and/or levels, it will essentially get embedded/spread into a larger number of frequencies and scales, which can increase robustness.

Another suggestion for future work is to use more complex, more adaptive, and/or more rigorous HVS models specifically designed or adapted for wavelet/multiwavelet coefficients compared to the empirical model used in this research.

Another possible area of future research can include looking at quantisation models and methods used in wavelet based compression algorithms to determine the visual relevance of each coefficient.

Finally, a future study can investigate how to enhance the ideas presented in this thesis to enable the watermarking scheme to cope with other types of geometrical attacks, such as affine transforms and/or to cope with combined RST attacks. Similarly, the ideas presented in this research can be extended for use in video watermarking as well.

References

[1] A. Reddy & B. Chatterji, "A new wavelet based logo-watermarking scheme," Pattern Recognition Letters, vol. 26, no. 7, pp. 1019-1027, 2005.

[2] I. Cox, M. Miller, and J. Bloom, "Watermarking applications and their properties," In Proc. International Conference on Information Technology: Coding and Computing, 2000.

[3] "Digital Rights Management Market by Application (Mobile Content, Video on Demand, Mobile Gaming, eBook, others), by End User (SME and Large Enterprises), by Deployment (On-Premise and On Cloud) by Industry, and by Region - Global Forecast to 2020", TC 3829, October 2015.

[4] G. Bhatnagar, J. Wu, and P. Atrey, "Robust logo watermarking using biometrics inspired key generation," Expert Systems with Applications, vol. 41, no. 7, pp. 4563-4578, 2014.

[5] F. Hartung & M. Kutter, "Multimedia watermarking techniques," Proc. IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.

[6] M. Barni & F. Bartolini, Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications, New York, NY, USA: Marcel Dekker, 2004.

[7] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and Steganography, 2nd Edition, San Mateo, CA, USA: Morgan Kaufmann, 2007.

[8] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673 – 1687, 1997.

[9] F. Hartung, J. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," Electronic Imaging, pp. 147-158, 1999.

[10] B. Chen & G. Wornell, “Quantization index modulation methods for digital watermarking and information embedding of multimedia,” J. VLSI Signal Process., vol. 27, no. 1-2, pp. 7-33, 2001.

[11] P. Moulin &. A. K. Goteti, “Block QIM watermarking games,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 3, pp. 293-310, Sept. 2006.

[12] L. Pérez-Freire & F. Pérez-González, “Spread-spectrum vs. quantization-based data hiding: misconceptions and implications,” Electronic Imaging, pp. 341-352, 2005.

[13] H. Nyeem, W. Boles, and C. Boyd, “Digital image watermarking, its formal model, fundamental properties and possible attacks,” EURASIP Journal on Advances in Signal Processing, vol. 1, pp. 1 – 22, 2014.

[14] A. Piper & R. Safavi-Naini, “How to compare image watermarking algorithms,” Transactions on Data Hiding and Multimedia Security IV, pp. 1-28, 2009.

[15] I. Cox, M. Miller, J. Fridrich, and T. Kalker. Digital watermarking and Steganography, 2nd ed. Elsevier, Burlington, 2007.

[16] J. Lewis, “Fast Normalized Cross-Correlation,” Industrial Light & Magic, vol. 10, no. 1, pp. 120 – 123, 1995.

[17] S. Lee & S. Jung, “A survey of watermarking techniques applied to multimedia,” In Proc. International Symposium on Industrial Electronics (ISIE 2001), vol. 1, pp. 272-277, 2001.

[18] M. Grgic, K. Delac, and M. Ghanbari, Recent Advances in Multimedia Signal Processing and Communications, Springer, 2009.

[19] I. Cox, L. Miller, and J. Bloom, “Watermarking applications and their properties,” In Proc. of International Conference on Information Technology: Coding and Computing, pp. 6-10, 2000.

[20] B. Ram, "Digital Image Watermarking Technique using Discrete Wavelet Transform and Discrete Cosine Transform," International Journal of Advancements in Research and Technology, vol. 2, no. 4, 2013.

[21] P. Parashar and R. Singh, "A survey: Digital image watermarking techniques," International Journal of Signal Processing, Image Processing, and Pattern Recognition, vol. 7, no. 6, pp. 111 – 124, 2014.

[22] V. Solachidis and I. Pitas, "Optimal detector for multiplicative watermarks embedded in the DFT domain of non-white signals," EURASIP Journal on Applied Signal Processing, pp. 2522-2532, 2004.

[23] D. Cui, "Dual digital watermarking algorithm for image based on fractional Fourier transform," In Proc. Pacific-Asia Conference on Web Mining and Web-based Application, pp. 51-54, 2009.

[24] M. Suhail, M. Obaidat, S. Ipson, and B. Sadoun, "A comparative study of digital watermarking in JPEG and JPEG 2000 environments," Information Sciences, vol. 151, pp. 93-105. 2003.

[25] C. Chou and K. Liu, "A Perceptually Tuned Watermarking Scheme for Colour Images," IEEE Transactions on Image Processing, vol.19, no.11, pp. 2966 - 2982, Nov. 2010.

[26] G. Bhatnagar and B. Raman, "Encryption based robust watermarking in fractional wavelet domain," Recent Advances in Multimedia Signal Processing and Communications, pp. 375-416, 2009.

[27] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121-128, 2002.

[28] G. Strang & T. Nguyen. Wavelets and filter banks. SIAM, 1996.

[29] M. Vetterli & C. Herley, "Wavelets and filter banks: Theory and design," IEEE transactions on signal processing, vol. 40, no. 9, pp. 2207-2232, 1992.

[30] S. Mallat, "Multiresolution approximation and wavelets," Technical Report, Department of Computer Information Science, University of Pennsylvania, Philadelphia, PA, Sept. 1987.

[31] S. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 11, no. 7, pp. 674 – 693, 1989.

[32] Y. Meyer, "Ondelettes," vol. 1 of Ondelettes et Operateurs. Paris: Hermann, 1990.

[33] S. Shen, "Discrete Wavelet Transform," Lecture Notes, University of Maryland, Baltimore County, 2004.

[34] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A secure, robust watermark for multimedia," in Proc. 1st Int. Workshopon Information Hiding, R. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, pp. 185–206, Springer, May/June 1996.

[35] J. Smith and B. Comiskey, "Modulation and information hiding in images," In Proc. Workshop on Information Hiding, Ross J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, pp. 207–226, Springer, Isaac Newton Institute, University of Cambridge, UK, May/June 1996.

[36] I. Cox & M. Miller, "The first 50 years of electronic watermarking," EURASIP Journal on Advances in Signal Processing, vol. 2, pp. 126 – 132, 2002.

[37] R. Schyndel, A. Tirkel, N. Mee, and C. Osborne, "A digital watermark," in Proc. International Conference on Image Processing, vol. 2, Austin, TX, pp. 86–90, 1994.

[38] R. Wolfgang, C. Podilchuk, and E. Delp, "Perceptual watermarks for digital images and video," Proceedings of the IEEE, vol. 87, no. 7, pp. 1108-1126, 1999.

[39] N. Nikolaidis & I. Pitas, "Robust image watermarking in the spatial domain," Signal Processing, vol. 66, no. 3, pp. 385-403, 1998

[40] G. Bhatnagar, W. Wu, and B. Raman, "A new robust adjustable logo watermarking scheme," Computers & Security, vol. 31, no. 1, pp. 40 - 58, 2012.

[41] N. Sharma and K. Sharma, "A Modified LSB Technique of Digital Watermarking in Spatial Domain". arXiv preprint arXiv:1303.7353, 2013.

[42] J. Wang, H. Peng, and P. Shi, "An optimal image watermarking approach based on a multi-objective genetic algorithm", Information Sciences, vol. 181, no. 24, pp. 5501-5514, 2011.

[43] J. S. Tsai, W. B. Huang, and Y. H. Kuo, "On the selection of optimal feature region set for robust digital image watermarking," IEEE Transactions on Image Processing, vol. 20, no. 3, pp. 735-743, 2011.

[44] J. Abraham & V. Paul, "An imperceptible spatial domain colour image watermarking scheme," Journal of King Saud University-Computer and Information Sciences, 2016.

[45] Q. Cheng and T. Huang, "Robust optimum detection of transform domain multiplicative watermarks," IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 906 – 924, 2003

[46] H. Golestani, M. Joneidi, and M. Ghanbari, "Logo watermarking with unequal strength for improved robustness against attacks," In Proc. International Symposium on Telecommunications (IST), pp. 827-832, 9-11 Sept. 2014.

[47] W. Wu & G. Ren, "A DCT-based robust image watermarking using local moment," In Proc. International Conference on Data Mining and Intelligent Information Technology Applications, Macao, pp. 122-126, 2011.

[48] A. Yuliani & D. Rosiyadi, "Copyright protection for color images based on transform domain and luminance component," In Proc. Information Technology Systems and Innovation (ICITSI), pp. 1-4, 2016.

[49] A. Bhatti, S. Nahavandi, Y. Frayman, "3D depth estimation for visual inspection using wavelet transform modulus maxima", Journal of Computers and Electrical Engineering, vol. 33, no. 1, pp. 48-57, 2007.

[50] A. Bhatti, and S. Nahavandi, "Stereo correspondence estimation based on wavelets and multiwavelets analysis," Stereo Vision, In Tech Education and Publishing, Vienna, Austria, pp. 27-48, 2008.

[51] M. Alghoniemy and A. Tewfik, "Geometric distortion correction in image watermarking," Electronic Imaging, 2000.

[52] T. Luo, G. Xing, and I. Shi, "Mutual information based watermarking detection in wavelet domain for copyright protection," In Proc. Asia-Pacific Trusted Infrastructure Technologies Conference, pp. 113-119, 2008.

[53] E. Mwangi, "A geometric attack resistant image watermarking scheme based on invariant centroids," in Proc. IEEE International Symposium on Signal Processing and Information Technology, 15 – 18 December 2007, pp. 190 – 193, 2007.

[54] V. Senthil, R. Bhaskaran, "Wavelet Based Digital Image Watermarking with Robustness against Geometric Attacks", In Proc. International Conference on Computational Intelligence and Multimedia Applications, vol. 4, 13-15 December 2007, pp. 89 – 93, 2007.

[55] N. Makbol, B. Khoo, and T. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," IET Image Processing, vol. 10, no. 1, pp. 34-52, 2016.

[56] C. Patvardhan, P. Kumar and C. V. Lakshmi, “Robust DWT based colour image watermarking scheme,” In Proc. National Systems Conference (NSC), Noida, pp. 1-6, 2015.

[57] J. Hu, Y. Shao, W. Ma, and T. Zhang, “A robust watermarking scheme based on the human visual system in the wavelet domain,” In Proc. International Congress on Image and Signal Processing (CISP), pp. 799 – 803, 2015.

[58] D. S. Chandra, “Digital image watermarking using singular value decomposition”, In Proc. Midwest Symposium on Circuits and Systems (MWSCAS'02), vol. 3, pp. 264–267, 2002.

[59] S. Lagzian, M. Soryani, and M. Fathy, “A new robust watermarking scheme based on RDWT-SVD”, International Journal of Intelligent Information Processing, vol. 2, no. 1, pp. 22-29, 2011.

[60] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, and S. Liu, “Colour image encryption by using Arnold transform and colour-blend operation in discrete cosine transform domains.” Optics Communications, vol. 284, no. 1, pp. 123-128, 2011.

[61] M. Naseem, I. Qureshi, & M. Muzaffar, “Robust watermarking for medical images resistant to geometric attacks,” In Proc. International Multitopic Conference (INMIC), pp. 224-228, 2012

[62] P. Yap, X. Jiang, A. Kot, “Two-dimensional polar harmonic transforms for invariant image representation,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 7, pp. 1259–1270, 2010.

[63] W. Lim, “The discrete shearlet transform: a new directional transform and compactly supported shearlet frames,” IEEE Transactions on Image Processing, vol. 19, no. 5, pp. 1166–1180, 2010.

[64] W. Zhang & X. Meng, "An improved digital watermarking technology based on QR code," In Proc. International Conference on Computer Science and Network Technology (ICCSNT), vol. 1, pp. 1004-1007, 2015.

[65] Z. Zhang, C. Wang, and X. Zhou, "Image watermarking scheme based on Arnold transform and DWT-DCT-SVD," In Proc. International Conference on Signal Processing (ICSP), pp. 805 – 810, 2017.

[66] N. Ma, Q. Zhang, and Y. Li, "Digital image watermarking robust to geometric attacks based on wavelet domain," In Proc. International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA), 2010

[67] M. Khalili, "DCT-Arnold chaotic based watermarking using JPEG-YCbCr," Optik-International Journal for Light and Electron Optics, vol. 126, no. 23, pp. 4367-4371, 2015.

[68] I. Ansari & M. Pant, "Multipurpose image watermarking in the domain of DWT based on SVD and ABC," Pattern Recognition Letters, 2017.

[69] D. Karaboga, "An Idea Based on Honey Bee Swarm for Numerical Optimization," vol. 200, Erciyes University, Engineering Faculty, Computer Engineering Department, Technical Report-TR06, 2005.

[70] P. Rasti, G. Anbarjafari, and H. Demirel, "Colour Image Watermarking based on Wavelet and QR Decomposition," Signal Processing and Communications Applications Conference (SIU), pp. 1-4, 2017.

[71] S. Jia, Q. Zhou, and H. Zhou, "A Novel Colour Image Watermarking Scheme Based on DWT and QR Decomposition," Journal of Applied Science and Engineering, vol. 20, no. 2, pp. 193 – 200, 2017.

[72] Q. Su, Y. Niu, G. Wang, S. Jia, and J. Yue, "Colour image blind watermarking scheme based on QR decomposition," Signal Processing, vol. 94, pp. 219-235, 2014.

[73] O. Jane, E. Elbaşi, and H. İlk, "Hybrid non-blind watermarking based on DWT and SVD," Journal of applied research and technology, vol. 12, no. 4, pp. 750-761, 2014.

[74] U. Rajput & N. Tiwari, "A novel technique for RGB invisible watermarking based on 2-DWT-DCT algorithm," 2015 Global Conference on Communication Technologies (GCCT), 2015, pp. 386-390, 2015.

[75] Z. Lin, L. Niu, and X. Jiang, "A method on digital watermarking image against geometric distortion," In Proc. International Congress on Image and Signal Processing (CISP), pp. 130-134, 2014.

[76] C. Harris & M. Stephens, "A Combined Corner and Edge Detector," In Proc. Alvey Vision Conference, 1988, pp. 147 – 151, 1988.

[77] C Wang, X. Wang, C. Zhang, and Z. Xia, "Geometric correction based color image watermarking using fuzzy least squares support vector machine and Bessel K form distribution," Signal Processing, vol. 134, pp. 197 – 208, 2017.

[78] D. Huttenlocher, G. Klanderman, and W. Rucklidge, "Comparing images using the Hausdorff distance," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, no. 9, pp. 850 – 863, 1993.

[79] P. Saravanan, M. Sreekara, and K. Manikantan "Digital Image Watermarking using Daubechies wavelets," International Conference on Signal Processing and Integrated Networks (SPIN), pp. 57 – 62, 2016.

[80] S. Fazli & M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," Optik-International Journal for Light and Electron Optics, vol. 127, no. 2, pp. 964 – 972, 2016.

[81] S. Kumar, N. Jain, and S. Fernandes, "Rough set based effective technique of image watermarking," Journal of Computational Science, vol. 19, pp. 121-137, 2017.

[82] J. Ruanaidh & T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," Signal processing, vol. 66, no. 3, pp. 303-317, 1998.

[83] C. Serdean, Spread spectrum-based video watermarking algorithms for copyright protection, PhD. Thesis, De Montfort University, 2002.

[84] M. Kutter & S. Winkler. "A vision-based masking model for spread-spectrum image watermarking," IEEE Transactions on Image Processing, vol. 11, no. 1, pp. 16-25, 2002.

[85] L. Zhu & L. Zhu, "Electronic signature based on digital signature and digital watermarking," International Congress on Image and Signal Processing (CISP), pp. 1644-1647, 2012.

[86] O. Prakash & A. Khare, "CT and MR Images Fusion Based on Stationary Wavelet Transform by Modulus Maxima," Computational Vision and Robotics, pp. 199-204, Springer India, 2015.

[87] E. Gerasimova et al., "A Wavelet-Based Method for Multifractal Analysis of Medical Signals: Application to Dynamic Infrared Thermograms of Breast Cancer," Nonlinear Dynamics of Electronic Systems, pp. 288-300, Springer International Publishing, 2014.

[88] S. Mallat. A wavelet tour of signal processing. Academic press, 1999.

[89] J. Lewis, "Fast Normalized Cross-Correlation," Industrial Light & Magic, 1995.

[90] W. Wang, Y. Liu, S. Li, H. Yang, and P. Niu, "Robust image watermarking approach using polar harmonic transforms based geometric correction," Neurocomputing, vol. 174, pp. 627-642, 2016.

[91] Z. Lu & X. Zhang, "Robust image watermarking based on the wavelet contour detection," IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005, vol. 2, pp. ii-1165, 2005.

[92] S. Mallat & W. Hwang, "Singularity detection and processing with wavelets," IEEE transactions on information theory, vol. 38, no. 2, pp. 617 – 643, 1992.

[93] P. Nes, "Edge-Detection in Signals using the Continuous Wavelet-Transform: Edge-Detection in Medical UltraSound Images," MSc Thesis, Norwegian University of Science and Technology, 2006.

[94] C. Li, C. Zheng, and C. Tai, "Detection of ECG characteristic points using wavelet transform," In IEEE Transactions on Biomedical Engineering, vol. 52, no. 1, 1995.

[95] R. Almeida, J. Martnez, S. Olmos, A. Rocha, and P. Laguna, "A wavelet-based ECG delineator: Evaluation on standard databases," IEEE Transactions on Biomedical Engineering, vol. 51, no. 4, 2004.

[96] M. Moazami-Goudarzi, M. Moradi, and S. Abbasabadi, "High performance method for electrocardiogram compression using two-dimensional multiwavelet transform," IEEE Workshop on Multimedia Signal Processing, pp. 1-5, 2005.

[97] S. Jayaraman, S. Esakkirajan, and T. Veerakumar. Digital Image Processing. Tata McGraw Hill Education Private Limited, 2011.

[98] V. Strela, Multiwavelets: Theory and Application, PhD. Thesis, MIT, 1996.

[99] H. Soltanian- Zadeh and K. Jafari-khouzani, "Multiwavelet gradind of prostate pathological images," Proceedings of SPIE Medical Imaging conference, San Diago, CA, Feb 2002.

[100] P. Zadeh & C. Serdean, “An evaluation of multiwavelet families for stereo correspondence matching,” International Conference on Digital Telecommunications (ICDT2011), Budapest, Hungary, pp. 41-45, 2010.

[101] C. Serdean, M. Ibrahim, A. Moemeni, and M. Al-Akaidi, “Wavelet and multiwavelet watermarking,” IET Image Processing, vol. 1, no. 2, pp. 223-230, 2007.

[102] V. Strela, P. Heller, G. Strang, P. Topiwala, and C. Heil, “The application of multiwavelet filterbanks to image processing,” IEEE Transactions on image processing, vol. 8, no. 4, pp. 548-563, 1999.

[103] Y. Zhang, C. Wang, and X. Zhou, “RST Resilient Watermarking Scheme Based on DWT-SVD and Scale-Invariant Feature Transform,” Algorithms, vol. 10, no. 2, 2017.